

# **Right to Privacy and Data Protection Laws in India: Balancing Rights and Managing Conflicts**

*Thesis submitted in fulfilment of the requirements for the Degree of*

**DOCTOR OF PHILOSOPHY**

By

**Sumedha Ganjoo**



**BENNETT**  
**UNIVERSITY**  
A TIMES GROUP INITIATIVE

Department of School of Law

**BENNETT UNIVERSITY**

(Established under UP Act No 24, 2016)

Plot Nos 8-11, Tech Zone II,

Greater Noida-201310, Uttar Pradesh, India.

Month- July Year- 2022

## DECLARATION BY THE SCHOLAR

I hereby declare that the work reported in the Ph.D. thesis entitled “**Right to Privacy and Data Protection Laws in India: Balancing Rights and Managing Conflicts**”

submitted at **Bennett University, Greater Noida, India**, is an authentic record of my

Work carried out under the supervision of **Dr. Garima Tiwari co-supervisor Dr. Suvir**

**Kapur**. I have not submitted this work elsewhere for any other degree or diploma. I am fully responsible for the contents of my Ph.D. Theses.

Signature of the Scholar

Sumedha Ganjoo

Department of School of Law

**Bennett University, Greater Noida, India**

Date: 19- July-2022

## SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the Ph.D. thesis entitled "**Right to Privacy and Data Protection Laws in India: Balancing Rights and Managing Conflicts**", submitted by **Sumedha Ganjoo** at **Bennett University, Greater Noida, India**, is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree or diploma.

(Signature of Supervisor)

(Signature of –Supervisor-2)

Dr. Garima Tiwari

Dr. Suvir Kapur

School of Law, Bennett University

School of Law, Bennett University

Date: 19- July-2022

Date: 19- July-2022

## LIST OF ABBREVIATIONS

A.P	Andhra Pradesh
AC	Appeal Cases
ADPA	Austrian Data Protection Act
AHAR	Association of Indian Hotels and Restaurants
AIR	All India Reporter
ALL ER	All England Law Reports
All.	Allahabad
ALLMR	All Maharashtra Law Reporter
Anr.	Another
APPI	Act on Protection of Personal Information
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
Art.	Article
ASEAN	Association of Southeast Asian Nations
B2B	Business to Business
B2C	Business to Consumer
BDSG	Buneshdateenschutzge
BPO	Business Process Outsourcing
Cal.	Calcutta
CCPA	California Consumer Privacy Act
CCTV	Closed-Circuit Television
CERT-IND	Computer Emergency Response Team India
CFPIA	California Financial Information Privacy Act
CIC Regulation Act	Credit Information Companies (Regulation) Act
CMIA	Confidentiality of Medical Information Act
COPPA	Children’s Online Privacy Protection Act
Corpn.	Corporation
CPPA	Canadian Consumer Privacy Protection Act
CrPC, 1973	Criminal Procedure Code, 1973
DDoS	Distributed Denial of Services
Del	Delhi
Del. L.R.	Delhi Law Review
DIPA	Data Protection Impact Assessment
DISHA	Digital Information Security in Health Care Act
doi	Date of Issue
DPA	Data Protection Act, 2018
DPD	Data Protection Directive
DPO	Data Protection Officer
DSG	Datenschutzgesetz
ECHR	European Convention on Human Rights
ed.	Edition
EHR	Electronic Health Record
et. al.	And others

etc.	Et cetera
EU	European Union
FADP	Federal Act on Data Protection
FCRA	Fair Credit Reporting Act
GDPR	General Data Protection Regulation
Guj.	Gujarat
HC	High Court
HIPAA	Health Insurance Portability and Accountability Act
I.L.R	Indian Law Reports
Ibid	Ibidem
ICCPR	International Covenant on Civil and Political Rights
ICO	Initial Coin Offering
Id.	Idem
ILI	Indian Law Institute
IPC, 1860	Indian Penal Code, 1860
IT	Information Technology
IT Act	Information Technology Act
ITAA	Information Technology Amendment Act
J.B.C.I	Journal of Constitutional and Parliamentary Studies
J.I.L.I	Journal of Indian Law Institute
JISSec	Journal of Information System Security
Jour.	Journal
JPC	Joint Parliamentary Committee
KPO	Knowledge Process Outsourcing
LGPD	Lei Geral de Protecao de Dados Pessoais
LPDP	Law on Personal Data Protection of Montenegro
LPO	Legal Process Outsourcing
Ltd.	Limited
M.P	Madhya Pradesh
Mad.	Madras
Media L.R	Media law Review
MeitY	Ministry of electronics and Information Technology
Mod.L.R	Modern Law Review
N.O.C	Notes of Cases
NALSA	National Legal Services Authority
NDA	Non-disclosure Agreement
NDHM	National Digital Health Mission
NYU	New York University
Ors.	Others
OTT	Over the Top
P&H.C	Punjab and Haryana High Court
Pat.	Patna
PCPNDTA	Pre-Conception and Pre-Natal Diagnostic Techniques Act
PDI	Personal Data or Information
PDP Bill, 2019	Personal Data Protection Bill, 2019

PDPA	Personal Data Protection Act, 2020
PDPL	Personal Data Protection Law, 2020
PDPO	The Personal Data (Privacy) Ordinance, 1996
PIL	Public Interest Litigation
PIPA	The Personal Information Protection Act
PIPEDA	The Personal Information Protection and Electronic Documents Act
PIPL	The Personal Information Protection Law, 2021
POPIA	The Protection of Personal Information Act
PPL	Protection of Privacy Law, 1981
PUCL	People's Union for Civil Liberties
Punj.	Punjab
Raj.	Rajasthan
Retd	Retired
RTI	Right to Information
S.C.J	Supreme Court Journal
SC	Supreme Court
SCALE	Supreme Court Almanac
SCC	Supreme Court Cases
SEBI	Security and Exchange Board of India
SMI	Social Media Intermediaries
SPDI	Sensitive Personal Data or Information
Supra	Above
T.N	Tamil Nadu
U.P	Uttar Pradesh
U.S	United States
UDHR	Universal Declaration of Human Rights
UIDAI	Unique Identification Authority of India
UK	United Kingdom
UNCITRAL	United Nations Commission on International Trade Law
UOI	Union of India
USA	United States of America
Vol	Volume
Vs./V.	Versus
W.L.R	Weekly Law Review

## LIST OF FIGURES

<b>Figure Number</b>	<b>Caption</b>	<b>Page Number</b>
1.1	Data protection framework in India	8
2.1	Ways of breach of privacy	2
2.2	Facets of privacy	3
2.3	Breach of Privacy as a Tort in Indian law	23
2.4	Remedies in Privacy	28
4.1	EHR Standards Coverage	70
6.1	E-mail to Grievance Officer	16
6.2	Automated reply	17
6.3	Automated Complain Form	17
6.4	Automated Response	18
6.5	Facebook Grievance Office	19
6.6	Amarchand Office	20
6.7	Mail to Amarchand	21

## LIST OF TABELS

<b>List Number</b>	<b>Caption</b>	<b>Page Number</b>
2.1	Case timeline on development of privacy law	20
4.1	Obligations of data fiduciary and grounds for processing of personal data without consent	11
4.2	Personal data and sensitive personal data of children	12
4.3	Data principle rights (rights of individuals whose personal data are processed)	14
4.4	Transfer of personal data outside India (norms for cross-border transfer of personal data)	15
4.5	Exemptions processing of personal data in the following categories shall not be permitted unless it is authorized by a law made by parliament and state legislature and is necessary for, and proportionate to, such interests being achieved	17
4.6	Penalties and compensation (remedies for unauthorized and harmful processing)	18
4.7	Offences (protect the autonomy of individuals in relation to their personal data)	19
4.8	Mandatory compliance under the IT Act and Rules made there under	30
4.9	Essential compliance though not mandatory	31
4.10	Other essential policies helpful in protecting data	34



## **CHAPTER-2**

### **PRIVACY- A GLOBAL RIGHT**

#### **2.1 INTRODUCTION:**

Privacy is the right to be free from covert observation and to select when, how, and to whom one's information is disclosed.<sup>1</sup> Privacy is an age-old concept and with time it has developed both in favor as well as against a person. Due to advancement in technology, its ambit has increased to include categories such as physical, informational, decisional and dispositional<sup>2</sup>.

The law has to keep pace with increase in advancement in technology to protect the rights of individuals. Several amendments in the existing statutes along with development and initiation of new statutes<sup>3</sup> have helped the Indian legal system to evolve<sup>4</sup>. The recent decision of the Supreme Court declaring privacy as a fundamental right has become a landmark judgement<sup>5</sup>.

#### **2.2 LAW OF PRIVACY**

The Information Technology Act, 2000<sup>6</sup> (hereinafter referred to as “IT Act”) under the definition of computer, a computer, computer system, computer network, data,

---

<sup>1</sup>Lindsey Norman, ‘An Overview of the Changing Data Privacy Landscape in India’ (2018) 919 <[www.pwc.in](http://www.pwc.in)>. Accessed on 2 November 2021.

<sup>2</sup>PayalThaorey, ‘Informational Privacy: Legal Introspection in India’ ILI Law, Review Vol and II Winter Issue (2019) II 160.

<sup>3</sup>Norman (n 1).

<sup>4</sup>Graham Greenleaf, ‘Data Protection: A Necessary Part of Indiaas Fundamental Inalienable Right of Privacy Submission on the White Paper of the Committee of Experts on a Data Protection Framework for India’ (2018) SSRN Electronic Journal.

<sup>5</sup>Commitee, ‘White Paper of the Committee of Experts on a Data Protection Framework for India’ (2017) White Paper

<[https://meity.gov.in/writereaddata/files/white\\_paper\\_on\\_data\\_protection\\_in\\_india\\_18122017\\_final\\_v2.1.pdf](https://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf)>.

Accessed on 22 March 2020.

<sup>6</sup>MA Yadugiri and Geetha Bhasker, ‘The Information Technology Act, 2000’ (2011)English Law 482.

computer database, and software are included.<sup>7</sup>The phrase encompasses broadly intrusions involving any electronic communication devices or networks, including mobile networks. The IT Act imposes civil responsibility and criminal punishment for a range of precisely defined computer-related acts, many of which directly or indirectly impair privacy.<sup>8</sup>

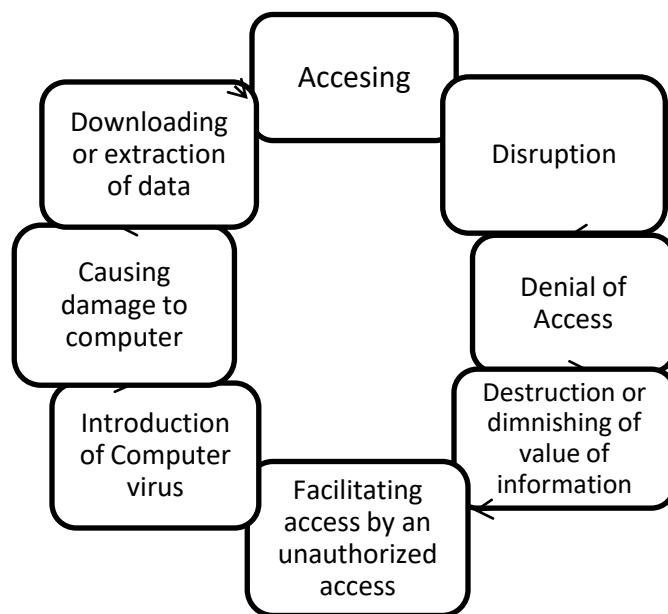


Figure 2.1: Ways of breach of privacy

The Act allows losses as recompense for damages caused by any of these activities. In addition, anybody who does any of these listed activities dishonestly and fraudulently is subject to imprisonment for a period of up to three years or a fine of up to five lakh rupees, or both.<sup>9</sup>

### 2.2.1 Facets of privacy

---

<sup>7</sup>ibid.

<sup>8</sup>Greenleaf (n 8)

<sup>9</sup>Yadugiri and Bhasker (n 6).

The modern scenario has led to the birth of multidimensional sphere to the concept of privacy protection. Therefore, there is a strong requirement to consider multifaceted nature of life as known to all, in order to develop a stringent privacy regime.



*Figure 2.2: Facets of privacy*

### **2.2.2 Bodily Privacy**

The foremost issue dealing with privacy is the physical protection of a person<sup>10</sup>. This facet of privacy can be seen and experienced in day-to-day life. Activities such as frisking at airports, narco-analysis tests come under the ambit of bodily privacy. The landmark case of **Selvi & Ors. vs. State of Karnataka**<sup>11</sup> is an example of such privacy.

Although the matter of privacy is constitutional, in case of criminal activities leading to violation of bodily privacy, the Indian Penal Code deals such cases under section such as;

1. Section 354C (voyeurism) which is an act like seeing and/or recording the image of a girl or woman moving through her private acts, where she feels that no one watches her. This involves a woman who is undressed or in her undergarments, or engaging in a sexual act, or who is using a toilet.

---

<sup>10</sup>Janet Zandy, 'Universal Declaration of Human Rights' (2019) 113 Radical Teacher 54.

<sup>11</sup> Selvi & Ors vs State Of Karnataka & Anr A.I.R 2010 S.C. 1974.

2. Section 354D (stalking)<sup>12</sup> It is unwelcoming and repetitive surveillance of another person by an individual or community. Stalking activities are attributed to stalking and coercion, and they can include following or watching the victim in person. In certain basic aspects, an offence like stalking is awful. Excessive stalking can result in serious emotional trauma for the victim. The accused can also move ahead to take bigger actions after stalking, thereby committing heinous offences such as murder or rape.

The need for bodily privacy is to protect the dignity of the individuals from any sort of attack with reasonable remedies.

### **2.2.3 Privacy related to personal life**

A person's family is his home, and his home is his world. This basic saying is to be considered while considering the privacy of a person in his own home. No person can intrude a man's personal space without legal backing or reasonable justification. However, there have been several instances in the past, in India and around the world, where people have violated this basic norm and infringed into a man's home. Media has a major role to play in such violation. From keeping updates about the location of a public figure to clicking them and their family's picture without consent. Such intrusion has even proved to be fatal for the families<sup>13</sup>.

It is essential that lawmakers understand this basic principle of privacy and develop reasonable and effective remedies against such violation of privacy.

### **2.2.4 Informational privacy**

---

<sup>12</sup>Tanaya Saha and Akancha Srivastava, 'Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization' (2014) 8 International Journal of Cyber Criminology 57.

<sup>13</sup>Cayce Myers, 'Digital Immortality vs. "The Right to Be Forgotten": A Comparison of U.S. and E.U. Laws Concerning Social Media Privacy' (2016) 16 Romanian Journal of Communication and Public Relations 47.

Information or data privacy is the privacy of personal information and usually related to personal data stored on computer systems. The need to maintain information privacy is applicable to collected personal information, such as medical record<sup>14</sup>, financial data, criminal records, political records<sup>15</sup>; business related information or website data<sup>16</sup>.

With the advancement in technology, every little detail of a person can be accessed easily online by any individual in the world. The recent case of privacy violation by **Facebook**<sup>17</sup> or the **UIDAI case**<sup>18</sup>, both have dealt with this matter.

Therefore, in order to protect the privacy of people related to their personal information such as banking records, health records, etc. formation of strict laws and their proper implementation and regulation is the need of the hour.

### **2.2.5 Communication privacy**

The sector which has seen maximum technological advancements is communication<sup>19</sup>. From a single landline phone in a locality to a smart phone in every individual's hand, the pace of technology development as well as affordability among the people has been rapid.

With the recent developments in the communication sector, interaction among people have increased manifold leading to very little personal privacy of citizens. Thus, in order to ensure individual as well as national security, lawmakers need to develop a

---

<sup>14</sup>Indian Medical Council, 'INDIAN MEDICAL COUNCIL (Professional Conduct, Etiquette and Ethics)' (2002) 2002 1 <[https://www.mciindia.org/documents/rulesAndRegulations/Ethics\\_Regulations-2002.pdf%0Ahttps://www.mciindia.org/CMS/wp-content/uploads/2017/10/Ethics-Regulations-2002.pdf](https://www.mciindia.org/documents/rulesAndRegulations/Ethics_Regulations-2002.pdf%0Ahttps://www.mciindia.org/CMS/wp-content/uploads/2017/10/Ethics-Regulations-2002.pdf)>. Accessed on 11 January 2020.

<sup>15</sup>Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity' (2005) 213 SSRN Electronic Journal.

<sup>16</sup>Greenleaf (n 4).

<sup>17</sup> Karmanya Singh Sareen And Anr vs Union Of India And Ors on 23 September, 2016 W.P.(C) 7663/2016 & C.M.No.31553/2016 (directions).

<sup>18</sup> 'Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India And Ors.' AIR 2017 SC 4161.

<sup>19</sup>Robert C Post, 'Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere' (2018) 67 Duke Law Journal 981.

legal framework that protects and safeguards individuals as well as ensures credible communication security<sup>20</sup>.

### **2.3 HISTORICAL BACKGROUND OF PRIVACY IN INDIA**

The existence of privacy can be found in many ancient texts of Ramayana<sup>21</sup>, Mahabharata<sup>22</sup>, Grihya – Sutras and Kautilya’s Arthashastra<sup>23</sup> “AVARANA” was used as a term which denotes existence of privacy “Avarana”<sup>24</sup> meant guard, shelter, or shield. It also meant that women need to keep her face covered under the veil. The concept of construction of houses originated from ancient Hindu text i.e., Grihya<sup>25</sup> Sutras.

Existence of the concept of privacy can be seen both in “Mahabharata” and “Ramayana<sup>26</sup>” where there were prefixed norms to be followed by human beings. These norms prohibited a man to see a sleeping woman, naked woman, to take woman alone, to enter someone’s house without permission. Kautilya Arthashastra<sup>27</sup> also prescribed all these norms to be followed, but also added the need and requirement of privacy at the time of confidential communication among the ministers.

In India there is a very famous saying “Sarva Seva Swagrihe Raja<sup>28</sup>” which means “Every man is the king of his own house”. In an Indian view this provides freedom to every man to behave, act and do whatever he/she wishes to and at the same time protects individual’s privacy within his/her household.

---

<sup>20</sup>Fahd AlDosari, ‘Security and Privacy Challenges in Cyber-Physical Systems’ (2017) 08 Journal of Information Security 285.

<sup>21</sup>Ralph TH Griffith,(1826-1906) ‘Translated into English Verse’.Ramayana

<sup>22</sup>Kisari Mohan Ganguli, (1883 and 1896) ‘The Complete Mahabharata in English.

<sup>23</sup>Medha Bisht, [2019] Kautilya’s Arthashastra.

<sup>24</sup>ibid.

<sup>25</sup>ibid.

<sup>26</sup>Griffith (n 21).

<sup>27</sup>Bisht (n 23).

<sup>28</sup>ibid.

When we talk about other religion prevailing in India, the existence of privacy can be seen in Islam, where peeping into other's house is strictly prohibited. Also, Hadith makes it reprehensible to read correspondence between others. In Christianity the text of Bible<sup>29</sup> clearly states, to live without interfering in the affairs of others. These examples make it clear that in India the concept of privacy has been prevailing from a very long time.

## **2.4 PRIVACY: THE INTERNATIONAL CHARACTER**

1. Article -12- Universal Declaration of Human Rights<sup>30</sup>
2. International Covenant on Civil and Political Rights 1966<sup>31</sup>
3. European Convention on Human Rights and Fundamental Freedoms 1950<sup>32</sup>

## **2.5 LEGAL INSTRUMENTS IN CONTEXT OF PRIVACY**

There are three major legal instruments where we need to identify the mention of Right to privacy:

1. International Legal Instruments: Drafted and formulated through United Nations.
2. Regional Legal Instruments: Instruments prepared in a particular region e.g.: American Convention<sup>33</sup>, European Convention<sup>34</sup>, African Charter etc.
3. Municipal Laws: Laws made / adopted / drafted by a particular country.
  - a) Common Law: Countries like U.K., U.S.A., India, Canada, Australia, South Africa falls under Common Law.
  - b) Civil Law: Countries like Germany, France and China follows civil law.

---

<sup>29</sup>Richard Challoner, 'The Holy Bible(1691-1781) - Douay-Rheims Version'.

<sup>30</sup>Hurst Hannum, 'The Status of the Universal Declaration of Human Rights in National and International Law' (1998) 3 Health & Human Rights 144.

<sup>31</sup>Martin Scheinin, 'The International Covenant on Civil and Political Rights', Making Treaties Work: Human Rights, Environment and Arms Control (2007)Cambridge University Press 323.

<sup>32</sup>CA Hopkins, 'European Convention on Human Rights' (1966) The Cambridge Law Journal 43.

<sup>33</sup>'American Convention on Human Rights.' (1987) Annual review of population law.

<sup>34</sup>M Duwell and D Mieth, 'The Charter of Fundamental Rights of the European Union' (2000) 5 Biomedical Ethics 51.

### **3.6 INTERNATIONAL INSTRUMENTS:**

#### **2.6.1 ANALYSIS OF UDHR 1948**

##### **2.6.1.1 ARTICLE – 12**

In this article different components of privacy have been mentioned but majorly it covers Individual Privacy.

In this article various components exist:

- a) Family Privacy
- b) Individual Privacy
- c) Home or correspondence Privacy
- d) Privacy related to honor and reputation.
  - There is prohibition of “arbitrary interference” under the right to privacy.
  - There is legal protection to the Right to privacy and various components mentioned therein.
  - There is specific protection to privacy rights against arbitrary interference or attack.
  - Major emphasis has been given to Individual Privacy under this Article.

#### **2.6.2 ANALYSIS OF INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS 1966.**

##### **2.6.2.1 ARTICLE-17<sup>35</sup>**

Article-17 is drawn on the same lines as that of Article 12 of UDHR.

The major difference between Article 12 (UDHR)<sup>36</sup> and Art-17 (ICCPR)<sup>37</sup> is the addition of the word “UNLAWFUL” in Article-17 which has elaborated the scope of Art-17 from Art-12.

---

<sup>35</sup>Scheinin (n 31).



Article 17 also gives major emphasis to individual privacy.

The Human Rights Committee has seen various reports under ART 40 and after going through them the committee has highlighted areas of concern. Few major concerns are as follows:

- a) Difficulty in protecting individual privacy from automated Information systems.
- b) Difficulty in protecting privacy from national intelligence services.

## **2.7 MAJOR REGIONAL LEGAL INSTRUMENTS PROTECTING RIGHT TO PRIVACY**

- a) The American Convention on Human Rights 1969<sup>38</sup>.

Article 11<sup>39</sup> of this convention talks about all other human rights along with Right to privacy as a civil and political right.

The first part of this article protects “honor” and “dignity” of every human being. Dignity is the most important ingredient to Individual Privacy.

- b) The African Charter on Human and People’s Rights, 1981<sup>40</sup>

Article 4<sup>41</sup> of the charter is indirectly applicable to the Right of Privacy.

It comprises of following components:

- (i) respect for life
- (ii) Integrity of a person
- (iii) Prohibition of any arbitrary deprivation of this right.
- (iv) Inviolability to humans

The concept of inviolability has been taken from Warren Brandeis’s<sup>42</sup> concept of inviolate personality. Inviolate personality<sup>43</sup> forms the major substance of Individual privacy that is how this article indirectly establishes Right to privacy.

---

<sup>36</sup> Gordon Brown ‘A Living Document and in a Changing World, The Universal Declaration of Human Rights in the 21st Century’(2016)NYU Global Institute of Advanced Studies 77.

<sup>37</sup>Scheinin (n 31).

<sup>38</sup>‘American Convention on Human Rights.’ (n 33).

<sup>39</sup>ibid.

<sup>40</sup>Michelo Hansungule, ‘The African Charter on Human and Peoples’ Rights’, The African Union: Legal and Institutional Framework: A Manual on the Pan-African Organization (2012)Brill 233.

<sup>41</sup>‘African Charter on Human and Peoples’ Rights.’ (1987).

c) Islamic Human Rights Instruments<sup>44</sup>

Those human rights instruments which are made based on the thoughts and beliefs of Islam can be categorized under Islamic Human rights instruments.

There are three major Islamic Declaration which includes right to Privacy.

- i) The Universal Islamic Declaration of Human Rights 1981 – Article 22 mentions Right to Privacy<sup>45</sup>.
- ii) The Cairo Declaration on Human Rights in Islam 1990 – Article 18 speaks about Right to Privacy<sup>46</sup>.
- iii) The Arab Charter on Human rights 2004 Article 21 gives Right to Privacy<sup>47</sup>.

The existence of Right to Privacy in the Islamic Declaration shows the importance of this right. This is because we can find existence of privacy in many Quranic Injunctions and the Declaration are largely based on these injunctions.

d) ASEAN Human Right Declaration 2012<sup>48</sup>

In ASEAN Human right Declaration Article 21 states that an Individual should have right to privacy. This article is formed in accordance with ART 12 of UDHR<sup>49</sup> and ART 17 of ICCPR<sup>50</sup>.

## 2.8 THE MUNICIPAL FRAMEWORK.

### A CRITIQUE OF COMMON LAW COUNTRIES

---

<sup>42</sup>Samuel D Warren and others, 'The Right to Privacy Today' (1929) 43 Harvard Law Review 297.

<sup>43</sup>ibid.

<sup>44</sup>Louise Saedén, 'Alternative Islamic Human Rights' (2010) Human Rights Studies 39 <<http://lup.lub.lu.se/luur/download?func=downloadFile&recordOid=1653579&fileOid=1670218>>. Accessed on 5 September 2019

<sup>45</sup>Zakia Belhachmi, 'The Universal Islamic Declaration of Human Rights', Women, Education, and Science within the Arab-Islamic Socio-Cultural History (2019) Brill 211.

<sup>46</sup>Susan Mumm Cairo Declaration on Human Rights in Islam, Religion Today: A Reader (2017) 1 Routledge 27.

<sup>47</sup>Rishmawi Mervat and Rishmawi Mervat, 'Arab Charter on Human Rights (2004), Max Planck Encyclopedia of Public International Law 97.

<sup>48</sup>"ASEAN Secretariat, 'ASEAN Human Rights Declaration and Phnom Penh Statement on the Adoption of the ASEAN Human Rights Declaration' 15 <[www.asean.org](http://www.asean.org)>."

<sup>49</sup>Zandy (n 10).

<sup>50</sup>Scheinin (n 33).

The common law countries rely on:

- a) Judicial decisions
- b) Statutory law
- c) Customary Practices
- d) Reasoning.

### **2.8.1 UNITED KINGDOM**

The originator of common law U.K. has been trying to develop law on privacy since 1948. That time there was no specific law on privacy and the decisions of these violations were based on breach of confidence.

Privacy was first considered as a breach of confidence before it got recognition as a breach of human rights through cases Von Hannover V. Germany (2005)<sup>51</sup>, PG and JH v. United Kingdom (2001)<sup>52</sup>. Through these cases the importance of privacy was realized and the need to protect and respect one's private life was thereby felt.

After this U.K. brought Human Rights Act 1998 to be in line with the European Convention on Human Rights.

When we draw a comparison on the laws of privacy in U.S.A. and U.K., we can see that privacy laws are not much advance and developed in U.K. as compared to U.S.A. U.S.A. enacted its privacy Act in the year 1974 whereas Human Rights Act 1998 and Data Protection Act, 1998 were first legislation enacted by U.K. for protecting privacy of individuals.

In the present era there are few statutory provisions passed by U.K., few provisions of which directly protects' Right to Privacy. Privacy laws have been passed in form of Parliamentary Initiatives, reports constitution and enactment's (statutory).

The above state laws are listed as follows:

- a) Privacy as a tort under Civil Law.

---

<sup>51</sup>Von Hannover v. Germany (2004) EMLR 379; (2005) 40 EHRR 1.

<sup>52</sup>P.G. and J.H. v. the United Kingdom (2001) 44787/98 .

- b) Law of Trust or Confidence
- c) The Wireless Telegraphy Act, 2006
- d) The Theft Act, 1968
- e) Private Members Bills, 1961-1970
- f) The Younger Committee Report, 1972
- g) The Rehabilitation of Offenders, 1974.

### The British Constitution

British has an uncodified constitution, due to which it is hard to look for privacy as a constitutional Right in U.K. The unwritten constitution is derived from different sources such as Acts of Parliament, Court judgments and conventions. Bill of rights, European Convention on Human Rights<sup>53</sup>, Fundamental Freedom 1950 and Human Rights Act, 1998 forms important source of legal system.

Though U.K. privacy law is well evolved as it is not based on any already written text, rather it is based evolving system of judicial decisions which makes it easy and flexible to give new meaning and dimensions to privacy with evolving times.

### **2.8.2 UNITED STATES OF AMERICA**

The Right to Privacy in United States of America was first recognized in Grisworld V. Connecticut (1965)<sup>54</sup>. Before this case an article was published by Harvard Law & Review authorized by Warren and Brandeis<sup>55</sup> in which privacy was defined as a “right to be left alone”.

After this Right to privacy was extended by the Supreme Court in Eisenstadt<sup>56</sup> where the right of unmarried couple to buy contraceptives was discussed. The Court said that the right to privacy recognised by the Constitution belongs to the individual, not the married couple.

---

<sup>53</sup>Hopkins (n 32).

<sup>54</sup>Griswold v. Connecticut, 381 U.S. 479 (1965).’

<sup>55</sup>Warren and others (n 42).

<sup>56</sup>Slobogin (n 16).

The Supreme Court further derived the concept of Right to privacy from Fourteenth Amendment<sup>57</sup> in the case of Roe<sup>58</sup>. In this case right to privacy was extended to include women's right to go for an abortion was discussed.

*Fourteenth Amendment's concept of personal liberty and restriction upon state action .....is broad enough to encompass a woman's decision whether to terminate her pregnancy<sup>59</sup>.*

In the case of Lawrence<sup>60</sup> fourteenth Amendment is further extended and the right to privacy included person of the same sex (who choose to) engage in ..... sexual conduct<sup>61</sup>. Based on fourteenth Amendment's guarantee of Due process court held the State cannot demean their existence or control their destiny by making their private sexual conduct a crime. Their right to liberty under the Due process clause<sup>62</sup> gives them full right to engage in their conduct without intervention of the government.

Therefore under U.S. Constitution though Right to Privacy is not explicitly protected but could be seen drawing its roots from First<sup>63</sup>, Fourth<sup>64</sup> and Fifth<sup>65</sup> amendments. Fourth Amendment<sup>66</sup> prohibits unreasonable searches and seizures whereas first and the fifth amendment includes privacy protections in that they focus not on what the govt. may do but rather on Individual's freedom to be autonomous.

---

<sup>57</sup>Authenticated U.S. Constitutional Information, 'Fourteenth Amendment: Rights Guaranteed Privileges and Immunities of Citizenship, Due Process and Equal Protection' 1559.

<sup>58</sup>Leon E Wein, 'The Responsibility of Intelligent Artifacts: Toward an Automation Jurisprudence' (1992) 6 Harvard Journal of Law & Technology 103.

<sup>59</sup>Authenticated U.S. Constitutional Information (n 57).

<sup>60</sup>ibid.

<sup>61</sup>Akhil Reed Amar, 'The Bill of Rights and the Fourteenth Amendment' (1992) The Yale Law Journal 48.

<sup>62</sup>Samuel Issacharoff, 'Due Process in Law', International Encyclopedia of the Social & Behavioral Sciences (2015) 2 Elsevier 696.

<sup>63</sup>John R Vile, David L Hudson and David Schultz, 'Federal Trade Commission' (2014) 131 Encyclopedia of the First Amendment 241.

<sup>64</sup>David Dorsen, 'Fourth Amendment: Search and Seizure' (2017) The Unexpected Scalia 61.

<sup>65</sup>ibid.

<sup>66</sup>ibid.

There is also Privacy Act of 1974<sup>67</sup> which guarantee individuals to access some government records files related to themselves. The government agencies keeping such records are prohibited from disclosing such information to any other party / person.

Here it is pertinent to discuss the law of tort and how it is an effective mechanism to handle privacy violations in U.S.A. When there is violation of privacy which is malice or atrocity lead by motives of gain, person can seek injunctive relief or recover damages. Tort prevents a person against emotional disturbances which can cause tension by his affairs and intimate life to public and by annoying and humiliating invasions of his solitude.

The right to privacy holds very strong foot in U.S.A. the legal and constitutional footing of privacy with the development of judicial decision given by Supreme Court is well developed to protect any kind of privacy violations.

The present situation of privacy in United States:

- (a) The U.S Constitution 1789.
- (b) Federal Privacy Laws:
  - The Privacy Act 1974<sup>68</sup>
  - Consumer Privacy Laws
  - Health and Medical Privacy Laws
  - Family Education Rights and Privacy Act, 1974<sup>69</sup>
  - Electronic Communication Privacy Act, 1986
  - Children's Online Privacy Protection Act, 2000
  - Neighborhood Children's Internet Protection Act, 2001.
  - The USA Patriot Act, 2001<sup>70</sup>.

---

<sup>67</sup>Bruce A Arrigo, 'Privacy Act of 1974', (2018)The SAGE Encyclopedia of Surveillance, Security, and Privacy 132.

<sup>68</sup>Arrigo (n 67).

<sup>69</sup>ibid.

<sup>70</sup>Tina Ebenger, 'The USA Patriot Act: Implications for Private E-Mail' (2008) Journal of Information Technology and Politics 771.

- The Federal Trade Commission, 2001<sup>71</sup>

(c) State Privacy Law: Privacy in workplace related laws.

The Right to privacy Act 1974<sup>72</sup> under the U.S. constitution has already been discussed. This act was passed to regulate government's action of collection, use, maintenance, and dissemination any personally identifiable information. This kind of information is correct and specific to identify a person. This could be name, address, home, or any other record.

This Act is based on Fair Information Practices<sup>73</sup> with following elements:

- a) Transparency
- b) Openness
- c) Review
- d) Correction
- e) Limitation over collection
- f) Accurate and complete
- g) Limited use
- h) Limit on transfer of Information

More or less in every sector law related to Privacy can be seen in United States. This makes their legal system advanced and developed.

## **2.9 THE HISTORICAL BACKGROUND OF INDIAN CONSTITUTION IN CONTEXT TO PRIVACY**

---

<sup>71</sup>Sanford Schwarz, 'Federal Trade Commission', *Research in International Economics by Federal Agencies* (2019).

<sup>72</sup>Arrigo (n 67).

<sup>73</sup>Post (n 20).

When the Constituent Assembly was debating on the preamble there was a lot of discussion with regards to Fraternity clause<sup>74</sup>, this shows the relevance and importance of dignity of an individual<sup>75</sup>.

The members of the Constituent Assembly<sup>76</sup> B. Pattabhi, Srimati Durga Bai, Thakurdas Bhargava, B.V. Keskar, T.T. Krishnamachari, M. Ananthasayanam and K. Sanathanam<sup>77</sup>wanted to change the language to the following order: -

Fraternity assuring the unity of Nation and the dignity of the Individuals<sup>78</sup>.

This proposal amendment was criticized and rejected on the ground that Unity of Nation<sup>79</sup> can only be achieved when dignity of individual is assured. Based on the lines of U.S. Constitution Fourth amendment Kazi Karimuddin forwarded an Amendment which was favored and supported by Dr. B.R. Ambedkar<sup>80</sup>. Though being convinced, Dr. Ambedkar supported it in a very reserved manner, due to which Right to Privacy was not incorporated in the constitution of India.

Even though this amendment related to the Constitution's 5<sup>th</sup> amendment, it was not accepted in full but a part of it was approved. It says the protection against self-incrimination given under Article 20(g)<sup>81</sup>. This Article is the essential clause to protect personal liberty. Confession made on own will, choice and freedom is very important and essential aspect of privacy. Therefore, it is the Privacy of Personal Liberty.

### **2.9.1 Constitutional Right to Privacy**

---

<sup>74</sup>Government of India, 'The Constitution of India: Selective Comments' (1993) Part IXA Constitution of India 1.

<sup>75</sup>ibid.

<sup>76</sup>Roy Kapoor, 'Constituent Assembly of India Debates ( Proceedings ) - Volume IX' (1949) IX.

<sup>77</sup>ibid.

<sup>78</sup>Government of India (n 74).

<sup>79</sup>Michael Gottlob, 'India's Unity in Diversity as a Question of Historical Perspective' (2007) Economic and Political Weekly 34.

<sup>80</sup>Shefali Jha, 'Secularism in the Constituent Assembly Debates, 1946-1950' (2002) Economic and Political Weekly 891.

<sup>81</sup>Ralph F Fuchs and PB Gajendragadkar, 'The Constitution of India' (1970) The American Journal of Comparative Law 331.



After the verdict in the case of *K.S. Puttaswamy v. UOI* the Right to privacy got its desired place under Article 21 of the constitution of India<sup>82</sup>. The scope of this extension under Article 21 came from the case of *Maneka Gandhi v. UOI* whereby the way of judicial activism and interpretation many human rights were made part of Article 21<sup>83</sup>.

If we look at the preamble, dignity of individual is already assured, and it has been already seen and discussed that privacy is an inseparable and integral part of human dignity. Therefore, this acceptance of human dignity in the preamble has already laid a ground for the development and incorporation of Right to Privacy in the Indian Constitution. Now after Right to Privacy becoming a fundamental right, right to live with human dignity has become very strong and forceful.

When we look deeper in the Indian Constitution, we can find other Articles which are providing Right to Privacy and protecting any violation against this right. One such article is Article 23 which prohibits trafficking, beggary etc. This article supports the concept laid down by Warren – Brandeis means inviolate personality. Article 23 also recognizes inviolate personality<sup>84</sup>.

Now that Privacy has become a fundamental right it can also be remedied by way of writ under Article 32 and 226<sup>85</sup>. The enforceability that has come to privacy after becoming a fundamental right has given this Right long due recognition.

Article 13 of the Constitution<sup>86</sup> is also essential when we talk about fundamental rights. This article clearly forbids the State from passing / making altering any law which is found to be in contravention to fundamental rights. Therefore, no act, regulation or law can contravene the right to privacy of an individual.

---

<sup>82</sup>ibid.

<sup>83</sup>ibid.

<sup>84</sup>A Berriedale Keith and GN Joshi, 'The New Constitution of India' (1939) The University of Toronto Law Journal 676.

<sup>85</sup>Michael C Dorf and Charles F Sabel, 'A Constitution of Democratic Experimentalism' (1998) Columbia Law Review 205.

<sup>86</sup>KC Wheare, 'The Constitution of India' (1951) International Affairs 403.

## 2.9.2 Judicial Development of Privacy

Year	Case	Ratio
1964	Kharak Singh v State of U. P. <sup>87</sup> .	<ul style="list-style-type: none"> <li>• Privacy is not a constitutional protection.</li> <li>• Article 21 (right to life) acknowledged the common law right to privacy and was the repository of residual personal rights.</li> </ul>
1975	Govind v State of M. P. <sup>88</sup> .	<ul style="list-style-type: none"> <li>• In any case, the right to privacy must be developed on a case-by-case basis.</li> <li>• Even granting that the right to personal liberty, the ability to travel freely across India's territory, and the freedom of expression generate an independent right of privacy that may be characterised as a basic right, we do not believe this right is absolute.</li> </ul>
1994	R. Rajagopal v State of Tamil Nadu <sup>89</sup>	<ul style="list-style-type: none"> <li>• The right to privacy is implied in Article 21's promise to the residents of this nation of the right to life and liberty. It is a “right to be let alone”.</li> </ul>
1997	People’s Union for civil Liberties v U.O. I <sup>90</sup> .	<ul style="list-style-type: none"> <li>• Article 21 of the Constitution protects the right to life and personal liberty, which includes the right to privacy.</li> <li>• Once the circumstances of each instance establish a right to privacy,</li> </ul>

<sup>87</sup>Kharak Singh v. The State of U. P. & Others, 1963 AIR 1295 .

<sup>88</sup>Gobind v. State Of Madhya Pradesh And Anr. on 18 March, 1975, AIR 1975 SC 1378..

<sup>89</sup> R. Rajagopal and Ors. v. State of Tamil Nadu, 1994 SCC (6) 632.

<sup>90</sup>People’s Union Of Civil Liberties v. Union Of India AIR 1997 SC 568.

		Article 21 applies. This right cannot be restricted unless in accordance with the legal process.
2005	District Registrar Collector, Hyderabad & Anr. v. Canara Bank & Anr <sup>91</sup> .	<ul style="list-style-type: none"> <li>• The right to privacy of an individual is distinct from the right to privacy of locations such as the house.</li> <li>• If anything is part of the public record, including court documents, the right to privacy cannot be asserted.</li> </ul>
2010	Selvi & Ors. v. State of Karnataka <sup>92</sup>	<ul style="list-style-type: none"> <li>• There must be a difference between the types of restrictions put on the right to privacy.</li> <li>• Although the ordinary exercise of police powers contemplates physical restraints such as the extraction of bodily substances and the use of reasonable force to subject a person to a medical examination, it is not feasible to extend these police powers to the coercive extraction of testimonial responses.</li> <li>• When conceiving the right to privacy, we must distinguish between physical privacy and the privacy of an individual's mental activities.</li> </ul>
2017	Unique Identification Authority of India & Anr. v. C.B. I <sup>93</sup> .	<ul style="list-style-type: none"> <li>• In an interim ruling, the Supreme Court ruled that the Unique Identification Authority of India may</li> </ul>

<sup>91</sup>Distt. Registrar & Collector, Hyderabad & Anr v. Canara Bank, AIR 2005 SC 186.

<sup>92</sup>Selvi and Ors. v. State of Karnataka, A.I.R 2010 S.C. 1974.

<sup>93</sup> Justice K.S. Puttaswamy and Anr. v. Union of India (UOI) and Ors, (2019) 1 SCC 1.

		not transmit the biometric information of any individual who has been assigned an Aadhaar number to any other agency without the individual's written agreement.
2017	Justice K S Puttaswamy (Retd.) v. U.O.I. & Ors <sup>94</sup> .	<ul style="list-style-type: none"> <li>• Privacy acknowledged as a basic right.</li> <li>• The concurring opinions of the judges in this case strengthened the right to privacy by recognising that it includes autonomy over personal decisions (e.g., consumption of beef), bodily integrity (e.g., reproductive rights), and the protection of personal information (e.g., privacy of health records).</li> </ul>

**Table 2.1:** Case timeline on development of privacy law.

The right to life protected by Article 21 has been expansively construed to include more than mere survival, simple existence, or animal existence.<sup>95</sup> Its scope is always expanding and thus refers to every aspect of a man's life. When the Constitution guarantees right to life, it also ensures right to live with dignity which can be ensured when the privacy of a person is maintained. Thereby, leading to the evolution and need of right to privacy.

Privacy enjoys a robust legal framework internationally. **Article 12 of the Universal Declaration of Human Rights, 1948**<sup>96</sup> and **Article 17 of the International Covenant**

<sup>94</sup> Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

<sup>95</sup> Government of India (n 77).

<sup>96</sup> Zandy (n 10).

**on Civil and Political Rights (ICCPR), 1966**<sup>97</sup>, legally protect persons against arbitrary interference with one's privacy, family, home, correspondence, honor, and reputation. India signed and ratified the ICCPR on 'April 10, 1979, without reservation. **Article 7 and 8 of the Charter of Fundamental Rights of the European Union, 2012**<sup>98</sup>, recognizes the respect for private and family life, home and communications. **Article 8** mandates protection of personal data and its collection for a specified legitimate purpose<sup>99</sup>.

The first mention of the right to privacy dates back to 1964 in the case of **Kharak Singh v State of UP**. The case involved the legality of certain police regulations that, without a statutory basis, authorised the police to keep under surveillance persons whose names were recorded in the history-sheet maintained by the police as habitual criminals or as persons who were likely to become habitual criminals. The petitioner alleged that this regulation led to violation of his fundamental right under **Article 19(1)(d)**<sup>100</sup> and personal liberty under **Article 21**<sup>101</sup>. The majority of the Supreme Court ruled that the regulation permitting police to perform house calls violated Article 21 of the Constitution. However, it did not violate Article 19(1). Ayyangar J. held that the right to privacy is not a right under our Constitution and therefore attempt to ascertain the movement of an individual which is merely a manner in which privacy is invaded is not an infringement of a fundamental right guaranteed by Part III.

Further, in **Gobind Singh v State of MP**, the court envisioned a right to privacy that comprised, among other things, the right to personal liberty, but affirmed laws identical to those overturned in the Kharak Singh case since they had legislative validity. In **R. Rajagopal v. State of T.N** the Supreme Court further explained right to privacy and held that it is the right to be let alone<sup>102</sup> and a citizen has the right to safeguard the privacy of

---

<sup>97</sup>Hannum (n 30).

<sup>98</sup>Duwell and Mieth (n 34).

<sup>99</sup>ibid.

<sup>100</sup>Government of India (n 77).

<sup>101</sup>ibid.

<sup>102</sup>Anja Mihr, 'Public Privacy - Human Rights in Cyberspace' (2013) SIM Working Paper 108.

his own and his personal relations. In its current status, the court has recognised the right to privacy as a basic fundamental right. The right forms an intrinsic part of Art. 21<sup>103</sup> and freedoms guaranteed under Part III. It permeates the core of preamble philosophy underlying liberty and dignity<sup>104</sup> as also human concepts of "life" and "personal liberty" enshrined in Article 21 and wide-ranging freedoms guaranteed under Part III<sup>105</sup>, considered essential for a meaningful human existence.

### **2.9.3 Privacy and Freedom of Speech**

**Article 19(1)(a)**<sup>106</sup> of the each and every person of India is guaranteed freedom of speech and expression under the Indian Constitution. It comprises expressing one's viewpoint orally or in writing. As freedom of speech and expression is essential for the spread of information on problems of public interest, so too is the protection of an individual's private life to the degree that it is unconnected to public obligations or concerns of public interest.

In cases concerning public figure or public officials, the dogged defense of the right to free speech is a constitutional obligation. The Indian Supreme Court held in the **Sahara India Real Estate Corpn. Ltd. v SEBI**<sup>107</sup>, that freedom of expression cannot be exercised at the altar of rights under Article 21 such as fair trial.

The ambit of freedom of speech also includes in it the freedom of press. In the present day and age, media plays an essential role in informing the people about anything and everything about anyone. An essential case in this regard is R. Rajagopal v State of T.N. The case dealt with the publishing of an autobiography of a prisoner, Auto Shankar, in the magazine Nakkheeran. Shankar was convicted of six murders and sentenced to death. Shankar authored his memoirs while incarcerated and requested that it be

---

<sup>103</sup>Government of India (n 77).

<sup>104</sup>ibid.

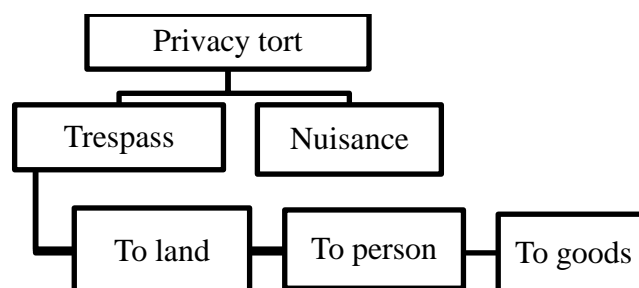
<sup>105</sup>ibid.

<sup>106</sup>ibid.

<sup>107</sup> Sahara India Real Estate Corporation Ltd &Ors vs. Securities & Exchange Board of India (SEBI) &Anr, (2013) 1 SCC 1

published in the petitioners' magazine. Before releasing his memoirs, Nakkheeran announced its impending release. Shankar was then compelled by prison authorities to compose a letter begging that the autobiography not be released. Petitioners filed this lawsuit to prevent respondents from breaching the magazine's and the prisoner's right to free speech. The court ruled that it was necessary to establish a balance between the freedom of the press and the right to privacy, and that the state and its officials do not have the authority to restrict the publishing of information that may discredit the state.

### 2.9.4 Breach of Privacy as a Tort in Indian law



**Figure 2.3**

#### **2.9.4.1 Trespass**

Trespass is the unlawful act of knowingly and directly causing damage to another's property. It is a deliberate act with the purpose to interfere with the property and person of another. The phrase purposefully connotes a deliberate act of wrongdoing. In addition, it is a required element of trespass to establish the purpose of the offending person.

- **Trespass to land** – Trespass to land refers to the wrongful interference of one over the property of another without any legal justification. It should be direct and physical. Trespass to land is more of a right over the

possession of property rather than ownership of property<sup>108</sup>. Thus, the individual in actual possession of the property may file a trespass to land claim against the property's owner. In the case of **Kesho Sahu v Muktakiman**<sup>109</sup>, the Patna High Court held in favor of privacy right which is albeit not inherent but is accorded by usage, grant or special permission.

- **Trespass to goods**- Trespass to goods refers to the inadvertent or purposeful interference with the property of another person without legal reason. Similar to trespass to land, trespass to goods may also be committed against the owner of the property.
- **Trespass to person** - Trespass to person refers to the situation in which a body or person is unlawfully apprehended. That is, there is a wrongful apprehension of one's body or person with the aim to do damage or injury.

#### 2.9.4.2 Appropriation

The tort of appropriation applies to the use for commercial purposes of an individual's likeness without any express consent on the part of such an individual.

The tort of appropriation, recognized in various jurisdictions in the United States, attempts to protect the identity of a person by affording rights to her name or likeness. Legislative recognition of this tort was granted in California, where its specific ingredients include:

- (a) The defendant's knowing use of the name, likeness or identification of the complainant
- (b) Without written permission from the appellant

---

<sup>108</sup>Rob Lucas, 'The Critical Net Critic' (2012) *New Left Review* 45.

<sup>109</sup>*Kesho Sahu v. Mt. Muktakiman*. AIR 1931 Pat 212



- (c) The defendant's commercial or other advantage
- (d) The plaintiff's damage.

However, the criteria of the Californian regulatory regulation are much stricter under common law than the traditional ingredients. Awareness on the part of the claimant is not only an additional ingredient in the tort regime, but it also demands that promotional usage to be specifically related to commercial promotion or paid advertising. It has been pointed out that the reason for this difference is that while the common law test seeks to protect the dignitary interest of a person, the status test aims to protect the dignitary interest of the individual.

Disputes about internet appropriation have become increasingly common place, however they mostly concentrate on the usage of a domain name that users can identify with another entity. From the above study, though, it is apparent that this tort may also be used to claim damages arising from some of the significant breaches of privacy at the hands of social networking platforms, particularly the now replaced. Facebook specifically used the names and photographs of customers in this service, which satisfies the 'name or likeness' provision of common law in the context of Facebook's own definition of the advertisement service, the additional constitutional requirement of information on the part of the complainant is thus readily met. However, the first problem area is with respect to the lack of prior agreement. Facebook may conveniently claim, taking recourse to its terms of use, that users have specifically allowed it to distribute user content for any commercial or promotional intent relating to the website. However, such an argument could be dealt with on the basis that Facebook's subsequent actions itself advertised the fact that it thought that further permission was required. Facebook, for example, has tried

Using the ten-second-long pop-up window to reinitiate the permission obtaining process (which never really afforded a true opportunity to make an informed choice). Mark Zuckerberg, Facebook's C.E.O., admitted this flaw himself and was cited as stating, "It took us too long after people began contacting us to change the product so that users had

to explicitly approve what they wanted to share." In addition, it was suggested that approval to any sharing in the sense of acquiescence to the terms of use of Facebook would not be immediately communicated. Finally, it is not very hard to prove that Beacon contributes to a market benefit since a user's endorsement serves as a company's word of mouth advertising and can be used by friends who may eventually have an interest in the product.

#### **2.9.4.3 Seclusion intrusions**

This applies to the act of human, electronic or mechanical interference into the life of a person and the information collecting procedure is adequate for this tort and no disclosure of the same is necessary. The intrusion tort is somewhat similar to the trespass tort, and the two are also concurrently claimed. An argument can be made to argue that whether he or she has a fair sense of privacy over that information, one cannot accumulate information about another.

#### **2.9.4.4 Private facts publication**

If a person is annoyed by having such personal information disclosed about him, this tort prevents a party from having facts (even if true) written. However, whether the complainant is encountered in a public location or if her actions are found to be newsworthy, the tort is inapplicable.

#### **2.9.4.5 Confidentiality Violation**

It has been argued that an impossible dream is chased by the above three privacy torts—that of complete privacy in which virtually no data that a person wishes to secure can be revealed to the outside world. However, it is a no brainer that at least a modicum of identity privacy is likely to be compromised in today's increasingly networked environment. The crime of breach of confidentiality is proposed in order to resolve this reality with a realistic approach.

This tort acknowledges that there will always be such violations of privacy and thus, reflects on the duties due within the chain of the violation. While the latter tort remedies

concentrate on the essence of the revealed information, breach of secrecy focuses on the nature of the relationship between the individual about whom the information is shared and the person to whom the information is shared. Here where the individual entitled to an obligation is in a position where it is already known or it should be known that the other person can fairly assume privacy rights, a duty of trust exists. For example, American courts have been hesitant to afford any security to credit card holders whose payment information is turned over to miscellaneous retailers by credit card firms on the basis that the credit card issuer has willingly provided the corporation with information and that the independent meaning of such information has not been recognized. Therefore, in a contemporary adaptation of *Duchess of Argyll v. Duke of Argyll*, whenever an unhappy ex-girlfriend shares personal or degrading information about her, it is recommended to apply the general rules of trust between users of social networking platforms inter-se. She could be dragged up under the tort of lack of faith by a Facebook boyfriend for the world to read and watch.

#### **2.9.4.6 Product Accountability**

In short, the principle of product liability provides that if one is engaging in the industry of manufacturing or otherwise delivering goods, delivers or distributes a faulty product, he is responsible for injury to individuals or property incurred by the defect. In the paradigm of product liability, there are many advantages of bringing anonymity to social networking sites. First, one of the consequences of enforcing an obligation on sellers to keep their goods safe is that sellers may be held responsible even though the accident is caused by the negligence of the buyer, provided that there is a bit-for and a proximate causal relation. Therefore, while Miss New Jersey may have been totally irresponsible in upgrading her new album's privacy settings as mentioned above, it would be assumed that Facebook should have predicted and covered against such an act of carelessness under the product liability regime. Another significant feature of product liability jurisprudence is that it is never possible to accept disclaimers as replacements for secure products. This is of great concern for social networking sites requiring consumer permission to disclaim any liability for harassment.

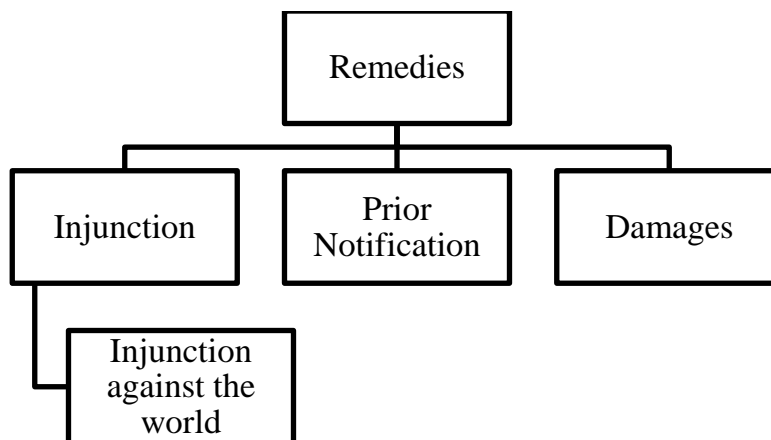


Figure 2.4 - Remedies in Privacy

## 2.10 Remedies in privacy actions

### 2.10.1 Injunction

It is an order of a court requiring a party to do or not to do a specified act or acts. In the case of **M. Gurudas v Rasaranjan**<sup>110</sup>, the Supreme Court summarized three factors to be considered by a court before grant of temporary injunction, 1. Prima facie case, 2. Balance of convenience, and 3. Irreparable loss. The Supreme Court in an earlier case recognized private law action for privacy as per the dictum of the Court. In *Douglas v. Hello Ltd*, it was determined that in situations involving prominent personalities or those who have made portions of their lives public, it does not always indicate that the relevant area of your private life is open to exploration or speculation by anybody who wishes to do so.

### 2.10.2 Injunction against the world

A super injunction is a kind of interim injunction, which is a temporary injunction granted before or during the commencement of proceedings, awaiting trial and ultimate judgement. The three aspects distinguishing super injunction from interim injunction are, 1. Super injunction is served upon third parties that are not impleaded as parties in

<sup>110</sup> M. Gurudas v. Rasaranjan (2006), AIR 2006 SC 3275

the proceedings along with the respondents of the injunction; 2. The proceedings may be anonymized and 3. Hearings will be conducted in private; access to court files can be restricted by a super injunction as well. In **Amar Singh v Union of India**<sup>111</sup>, the apex court granted an interim injunction against the world preventing publication of his allegedly taped telephonic conversations with multiple persons. However, due to petitioner's own misconduct in the case by virtue of application of doctrine of unclean hands led to vacation of the injunction.

### **2.10.3 Prior notification**

In case where an individual gives an advance notice before publishing any information related to a particular person, no action can be taken against him. However, this would enable the person to prevent the publication by an application for interim injunction.

### **2.10.4 Damages**

Damages of a fixed amount may be awarded to the plaintiff in case of pecuniary and non-pecuniary losses suffered. OK! Magazine was granted damages in the case Douglas v. Hello! Ltd for the income loss caused by the unlawful publishing of the plaintiff's wedding images by the defendant.

## **2.11 Statutory Laws/ Provisions related to Privacy**

There are number of statutes dealing with privacy either directly or indirectly. The comprehensive list of Statutory Laws is listed below: -

A) INDIAN PENAL CODE, 1860.

The most important section in IPC when we talk about Privacy is:

SECTION 509<sup>112</sup>

---

<sup>111</sup> Amar Singh Vs Union of India (UOI) and Ors, 2011 (7) SCC 69.

<sup>112</sup>Martha Nussbaum, 'Women and Equality: The Capabilities Approach' (1999) International Labour Review 66.

Through the Criminal Law (Amendment) Act 2013 this section has been amended to incorporate few changes to make this section stronger, punishment has been increased.

This section provides protection against the insult and invasion of a woman's modesty. This section is protecting the privacy of women by not allowing any sort of insult or intrusion upon her modesty.

Through Criminal Law (Amendment) Act 2013 new section has been added like Section 354A<sup>113</sup>, 354B<sup>114</sup>, 354C<sup>115</sup> and 354D<sup>116</sup>.

- Sexual Harassment is defined under Section 354A which is also punishable for the same offence<sup>117</sup>.
- The use of criminal force against a woman having intentions to compel her to get disrobed is mentioned under section 354B. This section also provides punishment for this offence<sup>118</sup>.
- VOYEURISM is defined under Section 354C<sup>119</sup>, it means receiving pleasure by seeing other person being involved in sexual activity or watching any women when she is naked. This is punishable under same section. This offence poses serious threat to Right to Privacy.
- Stalking is defined under Section 354D<sup>120</sup>. Stalking can be keeping an eye on the activity of a women, attempting to make a personal interaction without her interest.

---

<sup>113</sup>Scaria Kanniyakonil, 'New Developments in India Concerning the Policy of Passive Euthanasia' (2018) *Developing World Bioethics* 43.

<sup>114</sup>ibid.

<sup>115</sup>ibid.

<sup>116</sup>ibid.

<sup>117</sup>Ms Heena Keswani, 'Cyber Stalking: A Critical Study' (2017) *Bharati Law Review* 131 <<http://docs.manupatra.in/newslines/articles/Upload/455C1055-C2B6-4839-82AC-5AB08CBA7489.pdf>>. Accessed on 11 August 2021.

<sup>118</sup>Nidhi Arya, 'Cyber Crime Scenario in India and Judicial Response' (2019) 3 *International Journal of Trend in Scientific Research and Development* 1108.

<sup>119</sup>Abha Chauhan, 'Evolution and Development of Cyber Law - A Study with Special Reference to India' (2013) *SSRN Electronic Journal* 1.

<sup>120</sup>Keswani (n 117).

## B) THE INDIAN EVIDENCE ACT, 1872

This act has not overlooked privacy, rather it has tried to protect privacy in judicial proceedings. This act also protects privacy vs. various evidentiary interests.

Evidence Act also deals with Private documents under section 75<sup>121</sup>. These papers, as defined by this section, are those created by an individual in his private capacity for his private benefit. This is known as the Confidentiality of Documentary Evidence.

This act also provides for privileged communication under Section 122. The conversation between husband and wife during their wedlock is prevented to be presented or proved in court. This protects the privacy in a marriage.

Evidence Act provides informational privacy as well Section 123<sup>122</sup> States that no one can provide official unpublished records pertaining to any state. This section provides that such records can only be provided and that head of the department grants that permission.

Another provision is Section 125<sup>123</sup> which guarantee protection to person who informs about the commission of an offence. It is utmost important to preserve confidentiality by the public officer, so that there is no element of force with regards to the informant. This is an important provision in terms of law related to privacy.

Section 126 deals with confidentiality of communication under professional sphere. This section applies to legal practitioner and his client for example, this section is applicable to any fiduciary relationship based on trust. This section clearly indicates the importance of privacy under professional fiduciary relations under the evidence Act many provisions can be seen which are trying to protect

---

<sup>121</sup>Ari Ezra Waldman, 'Privacy, Trust, and the Propensity to Disclose' (2016) 67 SSRN Electronic Journal 41.

<sup>122</sup>ibid.

<sup>123</sup>ibid.

privacy. This act is comprehensive and effective enough when we think in terms of privacy.

### C) CRIMINAL PROCEDURE CODE, 1973

Under section 164(3), magistrate cannot compel a person who was committed an offence to make confession. His confession should be voluntary without any force. This is to protect the privacy as well as giving the person enough freedom to make his own choice. This section is based on Article 20<sup>124</sup> of Indian Constitution which protects against self-incrimination.

Criminal Procedure code also prohibits unreasonable search under Section 165(1)<sup>125</sup>. This section allows a person to enjoy his freedom and also protects privacy and security of a person. This section is based on Article 21<sup>126</sup> of the Constitution.

This code also protects privacy of rape victims during trials (proceedings). This code protects privacy of Individual in many ways.

### D) THE INDECENT REPRESENTATION OF WOMEN ACT, 1986

Section 2(c)<sup>127</sup> defines Indecent portrayal of women, which is the depiction of a woman's figure, shape, or body, or any portion thereof, in a manner that has the effect of being indecent or disparaging.

Another section of the act that is Section 3 prohibits the release of any advertisement or publication containing representation of women which is indecent.

---

<sup>124</sup>Wheare (n 97).

<sup>125</sup>'The Code Of Criminal Procedure' (n 110).

<sup>126</sup>Normawati Hashim, 'The Need for a Dynamic Jurisprudence of Right to "Life" Under Article 5(1) of the Federal Constitution' (2013) *Procedia - Social and Behavioral Sciences* 79.

<sup>127</sup>Debarati Halder, 'Examining the Scope of Indecent Representation of Women (Prevention) Act, 1986 in the Light of Cyber Victimisation of Women in India' (2013) *National Law School Journal* 112.



Section 4 prohibits sale, circulation .....etc. of any slide, book .....  
etc which depicts “indecent representation”.

This act protects privacy women and also prescribes punishment if indecent representation is made.

#### E) THE MEDICAL TERMINATION OF PREGNANCY ACT 1971

Terminating a pregnancy is a private affair for any woman of which she might not be comfortable disclosing it in public. Also, with the increase in rape cases and many minor girls who are undergoing with terminating their pregnancy is difficult to disclose such information in public. Any disclosure of such information is prohibited under Section 7(1)(c)<sup>128</sup>.

#### F) “THE PRE-CONCEPTION AND PRE NATAL-DIAGNOSTIC TECHNIQUES (Prohibition of Sex Selection) ACT, 1994”

When we talk about Right to Privacy of a woman, it’s the privacy of motherhood that is the most important. The problem of female feticide violates Right to life and also violates Right to Privacy of the mother. The violation of privacy is because of the pressure from the society to know the gender of the child and if there is a girl child abort her without the wish and will of the mother. This lowers the dignity of a woman and draws her status down into a mere animal existence<sup>129</sup>.

#### G) THE INDIAN CONTRACT ACT 1872

---

<sup>128</sup>Mohan Rao and Vina Mazumdar, ‘The Medical Termination of Pregnancy Act, 1971’, 2019 (The Lineaments of Population Policy in India 147 .

<sup>129</sup>Nithin Kumar and others, ‘Awareness and Attitudes Regarding Prenatal Sex Determination, Pre-Conception and Pre-Natal Diagnostic Techniques Act (PCPNDTA) among Pregnant Women in South India’ (2014) Journal of Clinical and Diagnostic Research.

The parties who are bound by a contract can only disclose information after obtaining due consent, in a defined manner for the defined purpose. If there is any disclosure of information in an unauthorized manner it would amount to breach of contract<sup>130</sup>.

When there is Data Processing contract or insurance contract it is paramount to maintain confidentiality and privacy under Section 73, 74 and 75<sup>131</sup>.

There is no privacy-specific clause in the Indian contract legislation, which establishes broad contract principles. However, we may discover privacy clauses in the interpretation of several provisions.

#### H) THE DIVORCE ACT 1869

In many matrimonial cases great amount of mudslinging can be seen. This can violate the privacy and cause embarrassment for the people who are party to such cases. To prevent such embarrassment there is provision in law to conduct in camera proceedings. Section 53<sup>132</sup> of this act lays down the same the principle behind this provision is to maintain privacy of the couple in marriage and after divorce.

#### I) INDIAN EASEMENT ACT, 1882

Easement law in India has been a customary law, which was also the first law to consider privacy as a right though in an indirect manner. The principles of building houses as mentioned in ancient literatures can also be found in medieval period as well has been seen to be based on privacy principles.

---

<sup>130</sup>Joseph Minattur, 'The Indian Contract Act: Its Wanderlust And Warmer Climes' (1972) Journal Of The Indian Law Institute 63.

<sup>131</sup>SHE F., Frederick Pollock and DF Mulla, 'The Indian Contract Act. With a Commentary, Critical and Explanatory' (1911) Harvard Law Review 107.

<sup>132</sup>Mishra N.N. and others, 'Privacy and Confidentiality: Beliefs, Expectations, and Protections in an Indian Context' (2012) Schizophrenia Research 117.

Section 18 of the easement act states that local custom should be seen while acquiring an easement. Since Right to Privacy has been part of customary easement privacy gets protection automatically.

#### J) THE INDIAN TELEGRAPH ACT, 1885

Section 5 gives the Central Government and State Governments the authority to order the interception of communications and seize licenced telegraphs in the event of a public emergency or threat to public safety.

This clause seems to be a violation since it bans trespassing and obstructing the telegraph office. Section 24<sup>133</sup> trying to know the content of messages” unlawfully. Section 25<sup>134</sup>, damaging and tempering Telegraphs intentionally.

The Telegraph Act is containing many provisions safeguarding and protecting privacy.

#### K) SPECIAL MARRIAGE ACT, 1954

There might be many cases where there is lot of mudslinging in those cases court can choose to have camera proceedings under Section 33 of this act.

#### L) THE HINDU MARRIAGE ACT, 1955

Section 22<sup>135</sup> of this Act also provides for camera proceedings.

#### M) THE CHILDREN ACT, 1960

---

<sup>133</sup>Ramesh Subramanian, ‘Security, Privacy and Politics in India: A Historical Review’ (2009) 6 Journal of Information Systems Security (JISSec) 567.

<sup>134</sup>ibid.

<sup>135</sup>Paras Diwan, ‘The Hindu Marriage Act, 1955’ (1957) International and Comparative Law Quarterly.

Under this act a special mention to be made is Section 36<sup>136</sup> which states that nondisclosure of address, name etc. of the child should be made in any news, report, article etc. which could lead to identification of child.

This Section is to protect the privacy of the child and is an important provision.

N) THE JUVENILE JUSTICE ACT (Care and Protection of Children) ACT, 2015.

Under this act, Section 3<sup>137</sup> lays forth specific requirements based on basic principles that must be adhered to by the central government, state governments, boards, and other entities.

Principle (xi) addresses the preservation of Juveniles' privacy.

Principle of Right to Privacy and confidentiality.

Every child shall have a right to protection of his privacy and confidentiality, and throughout the judicial process.

United Nations Convention on the Rights of the Child, 1989 has long back recognized right to privacy to be maintained for children. Due to which separate legislations has been adopted by U.S.A. and U.K.

Section 74 and Section 99 deals with privacy of a child.

O) RIGHT TO INFORMATION ACT, 2005

In a democracy, it is essential to have educated citizenry and information transparency in order to combat corruption and hold the government responsible.

---

<sup>136</sup>M Ramachandran and others, 'A Study on Juvenile Justice System in India before and after NIRBHAYA Case' (2018) 119.

<sup>137</sup>Smita Agarwal and Nishant Kumar, 'Juvenile Justice (Care and Protection of Children) Act 2015: A Review' (2016) 3 Space and Culture, India 5.

But in many cases this revelation of information can go against public need of preserving sensitive data. By enacting this Act democratic ideals are fulfilled but harmonizing these with the principles of Right to Privacy is important.

The constitution protects Right to Privacy, and it also guarantee Right to Information therefore Right to Privacy and RTI both holds a strong footing and must be protected against all odds with a perfect balance<sup>138</sup>.

#### P) THE CREDIT INFORMATION COMPANIES (REGULATION) ACT, 2005 (CIC REGULATION ACT)

The CIC Regulation Act provides that all credit information, companies can engaged only in one or more of the following businesses:

- Providing credit information to the credit report of individual and business borrowers.
- Offering data management services to its member Credit Institutions.
- Collecting, processing, compiling, and distributing data / information pertaining to mortgaged property held by credit institutions.
- Any additional role as stated by the Reserve Bank of India from time to time.

Data management services are described as the services of collecting, storing, developing systems for retrieving, aggregating, analysing, and distributing, publishing, and disseminating data, information, and other inputs to its members and designated users. And personal data refers to information on an identifiable individual, except the name, title, business address, or telephone number of a credit information firm employee.

Chapter VI of the CIC Regulation Act establishes some privacy rules and mandates that credit information businesses, credit institutions, and certain users adhere to them. The privacy principles provide:

---

<sup>138</sup>Law, Vol and Issue (n 2).

- (a) Manner and purpose of personal data collection: Personal data should not be acquired by a credit institution for inclusion in a publicly accessible publication unless it is for a permissible reason and is required or directly linked to that purpose.
- (b) Where a credit institution collects personal data for inclusion in a credit information report or a generally available publication, and such data is solicited from an individual concerned, the credit institution shall take reasonable steps before such data is collected or, if that is not practicable, as soon as practicable after such data is collected, to inform the individual of the intended use of the data.
- (c) Their level of responsibility: The credit information firm is responsible for any personal information in its possession or control, including data transmitted to a third party for processing. While the information is being handled by a third party, the credit information firm must offer a similar degree of security by contractual and other mechanisms.
- (d) Individuals may register complaints with the RBI against a credit information firm, a credit institution, or a particular user. The RBI is then authorised to either censure or apply any punishment it considers appropriate against the accused entity.

#### Q) THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016 (“AADHAR ACT”)

On March 3, 2016, the Aadhaar Act was tabled as a money bill in the Parliament. While opposing parties questioned its introduction (a money bill needs to be passed only in the Lok Sabha and Opposition parties claimed that since the BJP did not have majority in

the Rajya Sabha it sought to introduce this statute as a money bill). On March 25, 2016, the President of India granted his approval to the law, and on March 26, 2016, the Aadhaar Act was announced.

The purpose of the Aadhaar Act was to provide good governance, efficient, transparent, and targeted delivery of subsidies, benefits, and services where expenditures are incurred from the Consolidated Fund of India to individuals residing in India by assigning each person a 12-digit unique identification number, i.e., the Aadhaar number.

Section 3(1) of the Aadhaar Act stipulates that in order for a resident to obtain an Aadhaar number, he or she must provide "demographic information relating to the name, date of birth and other relevant information that may be prescribed but would not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history" and "biometric information photograph, fingerprint, iris scan or such other biological attributes of an individual that may be specified." At the time of enrollment, the Aadhaar Act mandates that the enrolling agency tell the person about how the information would be used. The nature of the recipients with whom the information will be shared during authentication, the existence of a right to access the information, the mechanism for requesting such access, and the name and contact information of the person or department to whom such requests may be directed.

Authentication is discussed in Chapter III of the Aadhaar Act. A person who intends to get a subsidy, benefit, or service is needed to validate his identity, provide evidence of Aadhaar number ownership, or enroll for an Aadhaar number. The Aadhaar Act mandates the establishment of a Central Identities Data Repository (which contains information on all Aadhaar number holders) and the Unique Identification Authority of India (Authority), which will authenticate the Aadhaar number of a holder upon request from a third party (Requesting Entity). Before collecting an individual's identity information ("defined as an individual's Aadhaar number, his biometric information, and his demographic information") for authentication, the Requesting Entity must obtain the individual's consent and ensure that the identity information is only submitted

to the Central Identities Data Repository for authentication. The Requesting Entity must also advise the person of the kind of the information that may be supplied following authentication, the potential uses of the information, and alternatives to providing identifying information to the Requesting Entity.

The Authority is required by Section 28 of the Aadhaar Act to protect the security and confidentiality of identification information and authentication records. The duty of the authority is to:

Adopt and execute suitable organisational and technological security measures:

Ensures that agencies, consultants, advisers, and other individuals tasked with carrying out any function of the Authority have implemented the necessary technological and organisational security measures.

Ensure that agreements/arrangements entered into with such agencies, consultants, advisers, or other persons appointed to perform any function of the Authority impose obligations equivalent to those imposed on the Authority by the Aadhaar Act and require such persons to act only on instructions from the Authority.

The Aadhaar Act further stipulated that core biometric information acquired or produced according to the Aadhaar Act could not be disseminated save for the restricted purpose of Aadhaar number production and authentication. The issue concerned a provision that permitted the sharing of identifying information other than core biometric information in line with the Aadhaar Act and in compliance with regulations. Under the IT Act and the regulations enacted there under, core biometric information is considered an electronic record and sensitive personal data or information.

The Aadhaar Act was criticised for several reasons, including its failure to address privacy and data protection concerns. The Aadhaar Act was challenged, and while downloading its decision, the Supreme Court of India ruled its legitimacy.

## **2.12 PRIVACY IN DIGITAL AGE**



### **2.12.1 The Information Technology Act, 2000**

Information Technology Act, 2000<sup>139</sup>, was passed by the Indian Parliament. It obtained the President's approval on 9 June 2000 and is effective as of 17 October 2000<sup>140</sup>. This Act is based on Resolution A/RES/51/162 adopted by the United Nations General Assembly on 30 January 1997 concerning the Model Law on Electronic Commerce, previously adopted by the twenty-ninth session of the United Nations Committee on International Trade Law (UNCITRAL)<sup>141</sup>.

The above United Nations resolution In light of the need for uniformity of the law applicable to alternatives to paper-based methods of correspondence and information storage, the General Assembly proposes that all states, when enacting or revising their rules, give favourable consideration to the Model Legislation on Electronic Commerce.<sup>142</sup>.

In the year 1997 alone, it was a foresight on the part of the Government of India to begin the whole process of enacting India's first ever IT legislation<sup>143</sup>.

Three explanations were given:

- (a) to promote the establishment of a stable regulatory atmosphere for electronic trading by supplying electronic contracting, protection and transparency of electronic transactions with a legal infrastructure;
- (b) to allow digital signatures to be used in authenticating electronic records; and

---

<sup>139</sup>Yadugiri and Bhasker (n 6).

<sup>140</sup>ibid.

<sup>141</sup>(UNCITRAL)., *Model Law on Electronic Commerce Guide to Enactment* (2001)

<[http://www.uncitral.org/pdf/english/texts/electcom/05-89450\\_Ebook.pdf](http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf)>. Accessed on 12 May 2022.

<sup>142</sup>ibid.

<sup>143</sup>Yadugiri and Bhasker (n 6).

(c) to demonstrate India's increasing IT capabilities and the government's role in safeguarding, encouraging and attracting FDI in the IT market.

It is necessary to note that the statutory aim was not to disregard the national or municipal (local) viewpoints on information technology when enacting the Information Technology Act, 2000, but to ensure that it could have an international viewpoint, as proposed by the UNCITRAL Model Legislation on Electronic Commerce<sup>144</sup>.

### **2.12.2 Key principles of the Act**

It is important to remember that the Indian Parliament provided a new legislative idiom for data security and privacy by the enactment of the Information Technology Act, 2000<sup>145</sup>.

The core data security and privacy standards enumerated under the 2000 Act on Information Technology<sup>146</sup> are:

- (i) concept of 'information,' database of computers,' information,' electronic medium,' originator,' address etc.
- (ii) Civil liability development if any party accesses or secures access to a computer, computer system or network of computers
- (iii) the establishment of criminal liability if any person accesses or secures access to a device, computer system or network of computers
- (iv) designation as a secure device of any computer, computer system or computer network
- (v) imposing a liability for breach of privacy and confidentiality
- (vi) the creation of a hierarchy of regulatory bodies, including the adjudicating officers, the Appellate Tribunal for Cyber Regulations, etc.

---

<sup>144</sup>(UNCITRAL)(n 141).

<sup>145</sup>Yadugiri and Bhasker (n 6).

<sup>146</sup>ibid.

### 2.12.3 The “Information Technology Act, 2000 And the Sensitive Personal Data or Information Rules”

The Information Technology Act, 2000<sup>147</sup> (“IT Act”) provides the law regarding protection of sensitive personal data or information (SPDI)<sup>148</sup>, the reasonable security practices and procedures for protecting such SPDI and punishment in case of wrongful disclosure and misuse of personal data. Section 43A<sup>149</sup> of the IT Act provides that if a body corporate that possesses, deals or handles any SPDI in a computer resource which it owns, controls or operates, is negligent in implementing and maintain reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain in any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected<sup>150</sup>. Explanation (ii) of the aforementioned section stipulates that appropriate security against unauthorised access, damage, use, modification, disclosure, or impairment, as may be defined in an agreement between the parties or as may be prescribed by law, should be provided. Moreover, the stated explanation stipulates that in the absence of such an agreement or regulation, the Central Government, in collaboration with such professional groups or associations as it deems appropriate, must regulate suitable security standards and procedures.<sup>151</sup>

Further, under Section 72A of the IT Act<sup>152</sup>, If a person reveals personal information in violation of a contract or without the agreement of the affected party with the purpose to cause or knowledge that disclosure is likely to cause wrongful loss or wrongful gain, he is subject to criminal penalties.

---

<sup>147</sup>Yadugiri and Bhasker (n 6).

<sup>148</sup>The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011’.

<sup>149</sup>Scott J Shackelford and Amanda N Craig, ‘Beyond the New “Digital Divide”’: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity’ (2014) 50 Stanford Journal of International Law 119.

<sup>150</sup>Norman (n 1).

<sup>151</sup>‘The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011’.

<sup>152</sup>Yadugiri and Bhasker (n 6).

#### **2.12.4 What is Sensitive Personal Data or Information<sup>153</sup>?**

The term sensitive personal data or information has been defined in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011<sup>154</sup>. SPDI Rules to mean such personal information which relates to:

- Passwords.
- Financial information such as bank account or credit card or debit card or other payment instrument details:
- Physical, physiological and mental health condition.
- Sexual orientation.
- Medical records and history; and
- Biometric information.

Any information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005 or any other law is not to be regarded as SPDI.

#### **2.12.5 Obligation on a Data Controller or Processor:**

- Privacy Policy<sup>155</sup> – SPDI Rules require that a person collecting, receiving, having, keeping, dealing, or handling information produce a privacy policy for handling or dealing in personal information, including SPDI, make it accessible to the suppliers of such information, and post it on their website. The privacy policy is expected to describe the kind of personal or sensitive personal data or information obtained, the objectives for collecting and using such information, the disclosure of information, and the acceptable security policies and procedures used.

---

<sup>153</sup>The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011’.

<sup>154</sup>ibid.

<sup>155</sup>James Grant, ‘International Data Protection Regulation’ (2005) 21 Computer Law & Security Review 257.

- Consent – The SPDI Rules<sup>156</sup> require written consent to be taken from the data subject and prohibit the collection of SPDI unless the same is necessary and for a lawful purpose. The SPDI Rules<sup>157</sup> provide that any disclosure of SPDI requires consent of the data subject.
- Grievance Officer – The SPDI Rules<sup>158</sup> require a grievance officer to be appointed by the organization and the contact details of such person to be specified in the privacy policy.

### 2.12.6 Transfer of Data

With respect to transfer of SPDI, an organization may transfer SPDI to any other body corporate or a person in India, or located in any other country, that (a) Provides the same degree of data protection as is mandated by the SPDI Rules and is adhered to by the body corporate.<sup>159</sup>, and (b) Only if the transfer is essential for the fulfilment of a legitimate contract with the data subject or if the data subject has agreed to the transfer may it be permitted.

### 2.12.7 Enforcement of the SPDI Rules<sup>160</sup>

There is no national regulator responsible for the enforcement of the SPDI Rules<sup>161</sup>. Claims for compensation of less than INR 50 million made under Section 43A of the IT Act are adjudicated by the Secretary of the Department of Information Technology of the relevant state government, while claims above INR 50 million are adjudicated by civil courts.

While the SPDI Rules<sup>162</sup> were significant when they were introduced and were a laudable step towards data protection. Given the pace at which technology, and the

---

<sup>156</sup>The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011’.

<sup>157</sup>ibid.

<sup>158</sup>ibid.

<sup>159</sup>ibid.

<sup>160</sup>ibid.

<sup>161</sup>ibid.

<sup>162</sup>Chakshu Roy and Harsimran Kalra, ‘Rules & Regulations Review’ <[http://www.prsindia.org/uploads/media/IT\\_Rules/IT\\_Rules\\_and\\_Regulations\\_Brief\\_2011.pdf](http://www.prsindia.org/uploads/media/IT_Rules/IT_Rules_and_Regulations_Brief_2011.pdf)>. Accessed on 13 February 2020.

world around us, is changing, there is a need for a stringent legal framework regulating data protection. This has been recognized in the Srikrishna Report<sup>163</sup> as well where the Expert Committee has commented on certain shortcomings of the “SPDI Rules”. These includes the definition of sensitive personal data as being unduly narrow, leaving out several categories of personal data from its purview, obligation not applicable to the Government and that on a strict reading. Section 43A of the IT Act<sup>164</sup> being overridden by contract.

### **2.12.8 3 Elements for establishing a violation of secrecy / Privacy**

The information is protected.

The information is shared under strict secrecy.

There must have been illegal use of the information to the plaintiff's harm.

## **2.13 THE ACT OF INFORMATION TECHNOLOGY, 2000 AND PRESERVATION OF PRIVACY: A REVIEW**

The Information Technology Act, 2000 is not law per se on data or privacy rights. It does not establish any data security or privacy rules. The Information Technology Act, 2000 is a comprehensive act that covers a variety of topics, including digital signatures, public key infrastructure, e-governance, cyber-contraventions, cybercrimes<sup>165</sup>, and privacy and confidentiality. It suffers from the syndrome of One Act.

The Information Technology Act, 2000 deals in a piecemeal manner with the topic of data security and privacy<sup>166</sup>. There is no actual regulatory mechanism that adequately tackles and protects data privacy problems in the context of a data protection regulator,

---

<sup>163</sup>Srikrishna Experts Committee, ‘A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians’ (2018) 2018 176 <[https://meity.gov.in/writereaddata/files/Data\\_Protection\\_Committee\\_Report-comp.pdf](https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf)>. Accessed on 22 June 2021.

<sup>164</sup>Fair Digital Economy, Protecting Privacy and Empowering Indians, ‘A Free and Fair Digital Economy Protecting Privacy , Empowering Indians Committee of Experts under the Chairmanship of Justice B . N . Srikrishna’.

<sup>165</sup>TN Varma, ‘Curbing Cyber Crimes by Indian Law’ (2017) SSRN Electronic Journal 94.

<sup>166</sup>Basant Kumar, Data Security and Privacy Management; Addressing Meticulous Crime Strategies in Smart Cities’ (2015) 3 22 <<http://www.recentscientific.com/sites/default/files/5456.pdf>>. Accessed on 17 September 2021.

data accuracy and proportionality, data accountability, etc. Even after amendment to the 2000 Act on Information Technology were implemented, India still lacks a real data security and privacy legislative system<sup>167</sup>.

### **2.13.1 Threat to privacy on Internet**

Use of Cookies, web bugs and trojans and other viruses to collect personal information.

- Cookies enable a website to identify you and remember your preferences.
- Advertisers deploy cookies to track user preferences.
- The information gathered by cookies is sold to third parties.
- A web bug is a graphic that exists on a website that enables a third party to monitor the person who reads a web page or an email message.

### **2.13.2 Right to Privacy Post Puttaswamy**

In Indian Jurisprudence, the 2017 Puttaswamy judgment reaffirmed the 'Right to Privacy' as a constitutional right. Since then, in many cases, it has been seen as an important precedent to stress the right to privacy as a human right and to explain the scope of it. The discussion on privacy has been re-ignited with the Personal Data Protection Bill tabled in 2019, and as such. After the Puttaswamy verdict, it is important to discuss the contours of the right to privacy as a fundamental right.

#### **2.13.2.1 Navtej Singh Johar and Ors Vs. Union of India (UOI) and Ors., 2018 (Supreme Court)<sup>168</sup>**

In this case, the Supreme Court of India unanimously ruled that **Section 377** of the Indian Penal Code 1860 (IPC)<sup>169</sup> was unconstitutional in that it criminalized consensual sexual behavior between adults of the same sex, criminalizing 'carnal intercourse against the order of nature. The petition challenged Section 377 on the grounds that it was

---

<sup>167</sup>Post (n 20).

<sup>168</sup>Navtej Singh Johar vs Union Of India Ministry Of Law And Justice AIR 2018 SC 4321.

<sup>169</sup>Joanne Shattock and Angus Easson, 'Chapter II.' (2018) The Works of Elizabeth Gaskell 207.

vague and violated the basic rights to privacy, freedom of expression, equality, human dignity, and immunity from discrimination granted by Articles 14, 15, 19, and 21 of the Constitution.<sup>170</sup>. In the case the Court relied on the judgment *Puttaswamy v. Union of India*, which holds that it would be violate of their human rights to refuse the LGBT community the right to privacy on the basis that they constitute a minority of the population, and that sexual orientation constitutes an intrinsic part of self-identity and refusing the same would be violate of the right to life.

#### **2.13.2.2 K.S. Puttaswamy and Ors Justice. Vs. India Union (UOI) and Ors., 2018 (Supreme Court)**

The Supreme Court upheld the legality of the Aadhar Scheme on the basis that because limited biometric data are obtained in the enrollment process and the verification process is not open to the public, it did not breach the right to privacy of people. The majority affirmed the constitutionality of the Aadhaar Act, 2016, save for a few clauses on private companies' disclosure of personal information, knowledge of crimes and use of the Aadhaar ecosystem<sup>171</sup>. As set out in the *Puttaswamy* (2017) decision, they focused on the fulfilment of the proportionality test.

#### **2.13.2.3 Joseph Shine vs. India's Union (UOI), 2018 (Supreme Court)<sup>172</sup>**

In this case the Supreme Court decriminalized adultery, questioning the substantive legitimacy of IPC Section 497 (adultery) and Section 198(2) of the Criminal Procedure Code, 1973 (CrPC). The Court holds that the state has placed its imprimatur on a man's power of his spouse's sexuality in criminalizing adultery, thereby failing to conform to the touchstone of Article 21<sup>173</sup> of the legislative clause. Section 497<sup>174</sup> was struck down on the basis that by embracing a notion of marriage that subverts true equality, it deprives a woman of her sovereignty, integrity and privacy and that it compounds the violation of her right to life and personal rights. In this situation, concomitant decisions

---

<sup>170</sup>Government of India (n 77).

<sup>171</sup>ibid.

<sup>172</sup> *Joseph Shine vs Union Of India*AIR 2018 SC 4898.

<sup>173</sup>Slobogin (n 16).

<sup>174</sup>Report No. 154 (The Code of Criminal Procedure, 1973 (Act No 2 of 1974) Vol II).Pdf.



referred to Puttaswamy to clarify the principles of sovereignty and dignity and their intricate relationship, as guaranteed in the Constitution, with the security of life and liberty. They relied on the Puttaswamy judgment to illustrate the risks of the use of privacy as a veneer for women's patriarchal dominance and abuse. They also cited Puttaswamy to explain that privacy is the right of any citizen, with no distinction to be made on the basis of the role of the individual in society.

#### **2.13.2.4 Association of Indian Young Lawyers and Ors. V. The State of Kerala and Ors., 2018, (Supreme Court)<sup>175</sup>**

In this case the Supreme Court affirmed the freedom to access the Sabarimala Temple for women aged 10 to 50 years. The court held that ultra vires (i.e. not approved under the Kerala Hindu Places of Public Worship (Authorization of Entry) Act, 1965) were Rule 3(b) of the Kerala Hindu Places of Public Worship (Authorization of Entry) Rules, 1965, which prohibits the entry of women into the Sabarimala temple. Centered on principles of purity and pollution as an affirmation of the inalienable integrity of each person, J. addresses the pledge against social exclusion. Puttaswamy was expressly appealed to by Chandrachud (in his concurrent judgment) to clarify integrity as a facet of Article 21. In the course of its claims, Amicus argued that the application of the exclusionary method compels women to disclose both their menstruation status and their age, which constitutes a coercive disclosure and so violates Article 21 of the Constitution of India's right to dignity and privacy.

#### **2.13.2.5 Vinit Kumar Vs. Central Investigation Bureau and Ors., 2019 (Bombay High Court)<sup>176</sup>**

Under section 5(2) of the Indian Telegraph Act, 1885 (Telegraph Act) and the balance between the needs of public safety and the right of privacy, this case deals with phone tapping and monitoring.

---

<sup>175</sup> Association of Indian Young Lawyers and Ors. v. The State of Kerala and Ors., (2019) 11 SCC 1.

<sup>176</sup>“Vinit Kumar v. Central Investigation Bureau, 2019 ALLMR (Cri) 5227.”

Section 5(2) of the Telegraph Act requires telephone messages to be intercepted in the event of a national emergency, or when there is a need for public protection. Such interception must conform to the procedural protections laid out in **PUCL v. Union of India (1997)**<sup>177</sup> by the Supreme Court, which were later codified as Telegraph Act laws. The Bombay High Court referred to the interception orders given under the Telegraph Act the tests of validity and proportionality carried out in *Puttaswamy*<sup>178</sup> and held that in this situation, the interception order could not be substantiated in the interest of public safety and did not conform with the test of the principles of proportionality and legitimacy as set out in *Puttaswamy*. The Bombay High Court annulled the surveillance orders in question and ruled that the copies/recordings of the correspondence intercepted should be deleted.

#### 2.13.2.6 **Supreme Court vs. Subhash Chandra Agarwal, 2019 (Supreme Court)**<sup>179</sup>

In this case the Supreme Court ruled that under the Right to Information Act, 2005 (RTI Act), the Office of the Chief Justice of India is a public authority allowing the disclosure of details such as personal belongings of the Judges.

In this case, notably in the *Puttaswamy* context, the Court has carefully explored the privacy implications of such disclosure. The Court found that there was an even footing between the right to know and the right to privacy and that there was no need to take the position that one right dominated over the other. The Court claimed that the proportionality test set out in *Puttaswamy* could be used by the Information Officer to balance the two rights, and also found that in the case of disclosure of personal information, the RTI Act itself had adequate procedural protections in place to satisfy this test. *X vs. Uttarakhand State and Ors, 2019* (Uttarakhand High Court).

The petitioner pleaded in this case that she had described herself as a woman and had undergone gender reassignment surgery and should thus be regarded as a woman.

---

<sup>177</sup>People's Union for Civil Liberties vs. Union of India & Ors AIR 1997 SC 568, (1997) 1 SCC 301.

<sup>178</sup>ibid.

<sup>179</sup>Supreme Court vs. Subhash Chandra Agarwal, 2019 (16) SCALE 40.

She was not regarded by the state as a person. While the Court relied largely on the **NALSA v. Union of India judgement of the Supreme Court**<sup>180</sup>, it also referred to the Puttaswamy judgment. The verdict specifically alludes to Puttaswamy's decision that the right to privacy is not intrinsically restricted to a single paragraph in the Fundamental Rights, but rather to an intersection of rights.<sup>181</sup> The fundamental right to privacy is defined by the intersection of Article 15 with Article 21 as an assertion of human autonomy, independence and identification. The Court also referred to the Supreme Court's judgement in **Navtej Singh Johar v. Union of India**<sup>182</sup>, which affirmed the petitioner's right to be recognized as a female on the grounds of all three judgments. (In light of the The Transgender Persons (Protection of Rights) Bill, 2019<sup>183</sup>, this judgment may need to be re-examined.)

#### **2.13.2.7 Association of Indian Hotels and Restaurants (AHAR) and Ors. Vs. The State of Ors and Maharashtra, 2019 (Supreme Court)**<sup>184</sup>

This case discussed the relevance of the **Maharashtra Obscene Dance Prohibition in Restaurants, Restaurant and Bar Rooms and the Preservation of Women's Integrity (Working therein) Act, 2016.**

The Supreme Court ruled that applicants for the issuance of a license should be deemed to be more objective and open-minded in such a manner that there is no full restriction on the staging of dance events at specified locations provided for in the Act. Several conditions were questioned under the Act, including one that allowed CCTV cameras to be placed in the rooms where dances were to be held. The Court relied here on Puttaswamy (and the dispute on unpopular privacy laws) to set aside the condition requiring such CCTV cameras to be mounted.

---

<sup>180</sup>National Legal Services Authority (NALSA) Vs. Union of India AIR 2014 SC 1863.

<sup>181</sup>Greenleaf (n 4).

<sup>182</sup>NALSA (n 180).

<sup>183</sup>Association of Indian Hotels and Restaurants (AHAR) and Ors. Vs. The State of Ors and Maharashtra, AIR 2019 SC 589

<sup>184</sup>The Gazette of India, 'The Transgender Persons (Protection of Rights) Act, (2019) Government of India Press 1.

**As a definition**, privacy requires what privacy means and how it can be valued. The degree to which privacy is a right includes privacy as a right (and should be legally protected). The statute does not specify what privacy is, but only what privacy situations will be given legal protection<sup>185</sup>. It is interesting to notice that a general right to privacy is not recognized by common law and the Indian Parliament has so far been hesitant to enact one.

The sense of the term is somewhat associated with secrecy and protection. Confidentiality requires a sense of 'expressed or' implicit ground for an individual concept of trust that is equitable. Privacy is the right of people, individuals, or organizations to decide for themselves where, if and to what degree knowledge about them is conveyed to others. The right to secrecy is something like a tacit duty. The right to let alone is the right.

The matter of secrecy occurs in the legal spoken word where a trust duty arises between a data collector and a data subject. This can occur from a number of situations or in relation to various categories of data that may be job, medical, or financial records. A duty of trust grants the data subject the freedom not to have his or her information used for other uses or released without his or her consent, unless there are other overriding grounds for this to be in the public interest.

An interest recognized and protected by moral or legal laws is also right. It is an interest, an infringement of which would be a legal error. Respect for such an interest would constitute a moral requirement. It is the universal principle of jurisprudence that there is a correlative obligation for every right and a correlative right for every duty. Yet there isn't an absolute law. In the context that a person may have a right but there may not be a correlative obligation, it is subject to such exceptions. Nevertheless, if privacy (and confidentiality) concerns are treated as 'rights along with obligations, it will be wise.

---

<sup>185</sup>Committee (n 5).

That is where information is provided for a reason other than the purpose for which it was issued.

## **2.14 COMPARATIVE STUDY OF PRIVACY LAWS IN U.S.A., U.K. AND INDIA.**

All the three countries hold different position in regard to laws on Privacy. Right to Privacy has many components as it is a multidimensional right, therefore the approach of all the three countries in regard to different dimension of privacy is different. Privacy is an elaborate right having different types, kinds, components etc. therefore it is difficult for any country to cover all components and the elements etc. of privacy.

When we talk about ancient history of Privacy, India had the strongest position of Privacy whereas U.S.A. and U.K. have no proof of any historical background to this right. If the laws related to privacy are compared in the present social scenario India is lacking far behind than U.K. and U.S.A.

For getting an in-depth understanding of Privacy protection laws lets draw a comparative analysis.

- a) Since ancient period India has recognized privacy as a customary right where in U.K. and U.S.A. privacy as a customary right was not recognized.
- b) Privacy as a customary right was recognized as statutory law in India in 1882 when Indian Easement Act 1882 was passed. The mention of privacy was found missing in the laws of U.S.A. and U.K.
- c) In terms of privacy as a tort, U.K. has recognized it under law of confidence. In U.S.A. William Prosser by way of judicial development made Privacy tort a separate tort. There is no existence of privacy tort in India.
- d) Article of Warren Brandeis<sup>186</sup> has originated the right to Privacy in U.S.A. In India it has been the case of Nuth Mull v. Zuka – Oollah Beg case 1855. Lastly in U.K. it was the case of Prince Albert v. Strange Case<sup>187</sup> which initiated the Right to Privacy.

---

<sup>186</sup>Warren and others (n 42).

- e) U.S.A. gives constitutional protection to Right to privacy, India also recognized Right to Privacy as fundamental right under Article 21. U.K. has an unwritten constitution therefore Right to Privacy as a constitutional right does not exist.
- f) India has incorporated Warren-Brandeis concept Right to Inviolate Personality<sup>188</sup> in form of Article 23 in Constitution of India. The mention of such provision is absent in U.K.
- g) There is no specific privacy legislation found in U.K. and India. The privacy provisions in both the countries are scattered in different legislations. But U.S.A. has enacted Privacy Act, 1974 which gives U.S.A. a comprehensive Privacy Protection law.
- h) India has not enacted any Health and Medical Privacy Laws whereas both U.K. and U.S.A. have enacted laws for the protection of privacy in Health and Medical regime.
- i) India is far behind in terms of enacting Data Privacy laws, there is a Personal Data Protection Bill, 2019 which is still in its draft stage. Whereas U.K. has enacted Data Protection Act and Human Rights Act in 1998, and in U.S.A. Privacy regime is oldest which started in 1974.

---

<sup>187</sup>Prince Albert v Strange: ChD 8 Feb 1849.

<sup>188</sup>Warren and others (n 42).

## **Chapter – 3**

### **3.1 GDPR- A Game Changer in Data Protection laws for the Digitalized World.**

The year 2012 heralded the beginning of 4 years of concentrated legislative efforts in the field of personal data protection in the EU that culminated into the EU voting for the implementation of the GDPR<sup>1</sup>, and finally lead to the publication of the GDPR in the Official Journal of the EU, in April 2016<sup>2</sup>.

The concept of personal data protection, however, was not a novel one. October 1995 witnessed the adoption of the EC Data Protection Directive (EC/95/46)<sup>3</sup> (the “DPD”). For years, the DPD continued to be the gold standard, as it were, in personal data protection lexicon.

So, what brought on the need for a new legislation, there were several factors that came into play. The DPD was felt to be archaic as technology had advanced in leaps and bounds since 1995. In the words of Elizabeth Denham, the UK Information Commissioner, Regardless of the rate of regulatory change, data-related technology advances more rapidly. Moreover, despite the fact that the EU Member States had transposed the DPD and the barriers to the free movement of personal data between the Member States had been removed, there were still too many legislative differences between the Member States, which led to disparities in how the DPD was implemented throughout the EU. Due to lack of adequately funded or resourced enforcement efforts, compliance to the DPD was “patchy” at best, causing multiple and increasing numbers of data breaches.” Data controllers took advantages of the above, and, therefore, business practices became more aggressive with personal data being

---

<sup>1</sup>“Microsoft, ‘Overview of the General Data Protection Regulation (GDPR)’ [2017] Information Commissioner’s Office <<https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>>.”

<sup>2</sup>Fair Digital Economy and others, ‘Introduction’ (2018) 4 European Data Protection Law Review 0 <<https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>>.

<sup>3</sup>Rebecca Wong, ‘The Data Protection Directive 95/46/EC: Idealisms and Realisms’ (2012) International Review of Law, Computers and Technology657.

misused/abused. Additionally, if one were to be honest, it seemed that the data subjects had very little actual control over the use of their personal data.

Overall, it was established that DPD in its current form would not last long. The weaknesses identified were, as follows<sup>4</sup>:

- Unclear linkage between "personal data" and actual privacy risks;
- The measures implemented to provide greater transparency were inconsistent and ineffective;
- The rules on international data export and transfer were archaic to say; the least;
- International data transfer was a cumbersome task;
- "Patchy" and "inconsistent" role of the Data Protection Authorities (DPAs);
- Other minor glitches that led to faulty implementation.

To address the aforementioned, it was felt that instead of completely overruling the DPD, it would be in everyone's best interests that the current arrangements be leveraged upon in a better manner, and that the current rules be implemented better. Pursuant to this, the first GDPR draft proposal was released in January 2012. In the following years, the draft was revised multiple times leading up to the final draft (in its present form) being eventually published in 2016.

Whilst Chinese astrologists might have been calling the year 2018 as the Year of the Dog, for a lot of people, 2018 proved to be the Year of the GDPR. May 25, 2018 — let's call it a watershed event in the history of data protection — witnessed the enforcement of the GDPR. In the months preceding and following May 25, 2018, we have seen the ripples of the stone inflicted by the GDPR globally, with EU Member States and other countries following suit in

---

<sup>4</sup>Douwe Korff, 'EC Study on Implementation of Data Protection Directive 95/46/EC' (2011) SSRN Electronic Journal 65.



transposing the GDPR into local legislation. Let us start with how the GDPR has apparently transformed the way we look at personal data protection.

### 3.2 GDPR versus DPD — a Sea-Change?

To the seasoned privacy practitioner, the changes do not seem too big. However, it would do us a whole lot of good to be wary of the GDPR, as there are significant changes and several new requirements<sup>5</sup>.

If it has to be summed up the changes brought on by GDPR whilst comparing it to the EU DPD:

- Increased territorial scope;
- More stringent consent obligations;
- New data subject rights;
- Increased accountability;
- Revisions to international data transfer;
- New legal liabilities;
- Significantly greater penalties.

All of the above translates into more onerous obligations on the part of data controllers and data processors, and a far more punitive enforcement regime when it comes to non-compliance with the GDPR.

This is captured below in an easy-to-read table:

Basis	<b>Data Protection Directive (DPD)<sup>6</sup></b>	<b>General Data Protection Regulation<sup>7</sup> (GDPR)</b>
-------	--	--

<sup>5</sup>Actiance, ‘GDPR Compliance and Its Impact on Security and Data Protection Programs’ (2017) IEEE Wireless Communications. 709

<sup>6</sup>Neil Robinson and others, ‘Review of the European Data Protection Directive’ (2009) Rand Europe Technical Report.

<sup>7</sup>Bocong Yuan and Jiannan Li, ‘The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation’ (2019) International Journal of Environmental Research and Public Health 551.

Wider Territorial Scope (or, the net is cast wide)	DPD applied to instances where personal data was processed within the EU or by using equipment located in the EU	GDPR, in addition to EU based companies, also applies to companies offering goods and services to EU citizens.
Holistic & Comprehensive (or, the cliched one-step shop)	Under the DPD, companies were answerable to the DPAs of the respective EU countries of establishment	In instances where the company has an EU office, the GDPR mandates a single supervisory authority (a lead DPA) in order to address data protection complaints across all EU Member States.
Consent (or, please make it a resounding YES)	In the era, personal data of subjects was obtained via implicit actions, opt-out boxes, and pre-ticked boxes.	Under the GDPR, the permission bar was raised and made much more stringent. Consent must be freely granted, particular, informed, unequivocal, and provided by explicit and affirmative action.
Penalties, (or, taking a punishment)	“Black points” under the DPD included both civil and criminal sanctions, forfeitures,	The GDPR imposes severe penalties, including fines of up to €20 million or 4% of a

	and fines up to EUR 250,000.	company's global annual revenue in the preceding financial year, whichever is greater.
Privacy by Design and by Default (privacy cannot be just a footnote)	Under the DPD, data protection and security mechanisms were unregulated, with privacy being a mere reference point.	Under the GDPR, companies will be required to embed privacy and data protection as a default action point into the initial designing of data processing activities.
Data Protection Officer (DPO) (or do you need a beat cop?)	Under the DPD, there was no mandate on whether a beat cop (read, DPO) should be appointed.	Mandate for Organizations/ companies carrying out processing of large-scale data of special categories to appoint and keep a DPO.
Data Controllers vs Data Processors (or as you sow, so shall you reap)	The DPD provided for a punitive regime for data controllers with data processors being out of bounds in most instances. Furthermore, if procedures were being followed, even data controllers were not considered liable for downstream (read,	The DPD stance now stands significantly transformed with the GDPR laying massive legal (and, more onerous) obligations at the door of the data processors. In fact, even data controllers will now be held liable for the non-compliance of

	service providers or data processors) processing errors.	data processors, in which they will have to pay the fines, whilst suing the data processor for damages caused)
Breach Notification Mandate (or, “give a bell”)	The DPD did not set forth express legal obligations to report data breaches. It did, however, indicate that serious data breaches be notified.	The GDPR mandates that in-scope companies report “high risk” breaches to regulatory authorities and data subjects within 72 hours of the breach coming to their knowledge.
Data subject Rights (“I here enhanced rights to my data now”)	The DPD set forth limited data subject rights, as follows: (1) limited right to erasure of PD – suppressed results of internet searches only. (2) right to access to personal data was ambivalent – no clear obligations on data controllers with regard to period and format of data to be given to the data subject; (3) no mention of data portability.	The GDPR makes data subjects rights broader and legally enforceable, as follows: (1) Rights of access. (2) Right to rectification (3) Right to erasures (4) Right to restrict processing (5) Right to object to processing. (6) Right to data portability.

--	--	--

### 3.3 The GDPR: An Analysis

The GDPR, without an iota of doubt, is an ambitious piece of legislation wherein the magnitude of predictable transformation is substantial. However, it does not have to be all Hydra-like, or the monster that it is largely perceived to be. Set forth here are some of the salient points that one must bear in mind while implementing privacy programs that are aligned to the GDPR<sup>8</sup>.

#### 1. Extraterritorial reach/nature of the GDPR

Although the GDPR fundamentally governs businesses set up in the EU; it also covers companies set up outside of the EU, offering goods and services to, or monitoring data subjects/individuals in the EU. Companies outside of the EU have to appoint a representative which has to be present in the EU (subject to limited exemptions), wherein the representative shall bear responsibility/liability for any breaches<sup>9</sup>.

#### 2. Core mandates around data protection are the same

The GDPR continues to be the same as the DPD in that the core mandate around processing of personal data are the same. It covers the acts of both data controllers and data processors. The 6 general principles of data protection make an appearance here as well, and companies must satisfy processing conditions/bases; however, there are significant new changes to the principles and the data processing conditions that one must be wary of. The definition of sensitive personal data is now expanded to include genetic and Homeric data.

#### 3. Consent

Consent continues to be one of the justifications for processing of personal data; however, valid consent is now harder to obtain. Moreover, data subjects can now withdraw consent at any point

---

<sup>8</sup>European Commission, 'Principles of the GDPR' (<https://ec.europa.eu/>, 2018) Accessed on 27 March 2020.

<sup>9</sup>Sangwoo Lee, 'A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing' (2019) SSRN Electronic Journal 233.

of time. Both in the case of sensitive personal data and for data transfers outside of the EU, explicit consent is required. With regard to provision of online services to a child, consent from a child will only be valid when authorized by a parent. The GDPR defines a child as a 16-year-old. This age can be reduced up to 13 years by Member States<sup>10</sup>. Additionally, there are more security provisions afforded to children, for example, the situations where the "legitimate interests" condition of processing may be used have been limited – this is to say that a child's "right to be forgotten" is now stronger and more fortified.

#### 4. Data subjects' rights

This is an area that has been brought to the forefront more than ever before with the implementation of the GDPR. While the existing rights relating to rectification of inaccurate data, objection to direct marketing, challenging automated decisions, etc., remain, there are several new and enhanced rights, like, the right to erasure (or, the right to be forgotten), the right to portability of data, etc<sup>11</sup>. These new rights are like knotted strands now, and a company will need to have proper response mechanisms in place to address these.

#### 5. Privacy notices

Privacy notices are now required to have multiple information points, as required by the GDPR, much more than before. One would think this would be case, but here's the quandary – bigger isn't necessarily better! Your notices will also have to simultaneously be concise and be able to make sense to the laymen<sup>12</sup>. It should skip the legalization and the jargon!

#### 6. Accountability

Being compliant or saying that you are complying is fine, but can you demonstrate compliance? Being able to demonstrate compliance means conducting privacy impact assessments where required (in cases of high-risk processing, especially), having adequate technical security measures in place, etc. In order to show that you are, indeed, compliant, you may even have to sign up to a code of practice or be certified.

---

<sup>10</sup>Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) *Information and Communications Technology Law* 108.

<sup>11</sup>PT Wolters, 'The Control by and Rights of the Data Subject under the GDPR' (2018) *Journal of Internet Law* 97.

<sup>12</sup>Mike Hintze, 'Privacy Statements Under the GDPR' (2019) *Seattle University Law Review* 796.

## 7. Data Protection Officers

Based on the kind of data processing that companies carry out, and the magnitude of their operations, they may be required to appoint a “data protection officer” (DPO). These DPOs are your subject matter experts in all aspects of data privacy and should be consulted for all data protection matters in the company<sup>13</sup>. DPOs are to report directly to the “highest level of management” within the company and cannot be penalized or terminated for doing their jobs.

## 8. Data security

GDPR suggests enhanced mechanisms like encryption, etc. Additionally, companies must pay heed to the data breach reporting requirements<sup>14</sup> (unless a breach is unlikely to cause a risk for individuals, companies must report data breaches to their supervisory authority “within 72 hours”).

## 9. Obligations of data processors

Right when data processors were sitting safely ensconced in their BPOs, call-centers, KPOs, LPOs, other IT structures, the GDPR decided to expand the list of obligations that these processors will have to bear the burden of, directly, and in their contracts with data controllers when it comes to claims by data subjects/individuals. Data processors can now be held jointly and severally liable along with data controllers<sup>15</sup>. Companies outside of the EU, who set themselves up as data processors earlier to escape such liability, can no longer plead innocence or ignorance.

## 10. International (outside the EU) data transfers

---

<sup>13</sup>Martin Brodin, ‘A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises’ (2019) European Journal for Security Research 343.

<sup>14</sup>Tony Ke and K Sudhir, ‘Privacy Rights and Data Security: GDPR and Personal Data Driven Markets’ (2020) SSRN Electronic Journal 114.

<sup>15</sup>Information Commissioner’s Office, ‘Overview of the General Data Protection Regulation (GDPR)’ (2017) Information Commissioner’s Office 412.

For data transfer outside of the EU, companies will have to ensure that certain conditions are met. Rules with regard to such international transfers<sup>16</sup> continue to remain tough to comply with. — There are some minor exemptions, but they aren't of much use, practically.

### **3.4 Decoding the GDPR Rubric**

In the countdown to May 25, 2018, and thereafter, the GDPR<sup>17</sup> continues to leave us and scratching our scalp. It might seem like a contagion to our collective imagination. How is one to survive the contagion communication of disease from one person or organism to another by close contact and its aftermath?

First step is to stop thinking of it as an epidemic, and instead, turn this into an opportunity to ensure that the data of individuals that is kept, and processed is secured at all times. This will change the way individuals and your holders look at you and will increase your brand value in the market. It's quite simple. Get your head out of the cloud of articles, blogs, commentaries about how difficult and cumbersome the GDPR is, and just think about the simple ways in which you can assure your employees, suppliers, clients, etc., that data is safe with you. Thinking about your stakeholders and not just the penalties imposed by the GDPR will make things a lot easier. As the data privacy experts at Linklaters put across quite succinctly: Privacy counsel will need a bit more consideration, a great lot of pragmatism, and a dash of bravery.

### **3.5 National Derogations**

One of the main drivers for the GDPR to come to the fore was the need to have an able and harmonious data protection framework across the EU. Hence, the GDPR is directly effective in all of the EU without the Member States having to

---

<sup>16</sup>Hiep Tran, 'Briefing on Data Processing and International Data Transfer in Accordance With GDPR' (2020) SSRN Electronic Journal 54.

<sup>17</sup>Sahar Bhaimia, 'The General Data Protection Regulation: The Next Generation of EU Data Protection' (2018) Legal Information Management 63.



implement national laws. However, there are, and will remain, several divergences, as there are so many elements of the GDPR that are bound by national legislation; we also have to bear in mind that different countries have varying cultural and social approaches towards data protection. Additionally, there are differences in the ways the different supervisory authorities will implement and enforce the GDPR in the respective Member States.

1. DPOs - it is up to Member States to make DPO appointment mandatory.
2. Children – Member States can reduce the age of consent (online services) for a child from 16 to 13 years old.
3. Employment – More stringent restrictions can be imposed by member states on processing of employee data.
4. National security – Member States can limit rights afforded to data subject/individuals in areas that concern national security, judicial proceedings, and crime.
5. Freedom of information - Member States can amend the GDPR so that the idea of data protection is reconciled with that of freedom of information. For example, Member States can restrict processing of national identity numbers, and protect information that is subject to professional secrecy.

Further, national law governs many processing activities. For instance, one of the bases for the processing of personal data happens to be to meet an obligation under Member State law; or that processing of information about “criminal offences” is only permitted when allowed by Member State law; or that the “right to be forgotten” does not apply if such processing is required by Member State law; or that a Member State recognized public interest can be used to transfer data outside of the EU and; that Member States can impose additional and more stringent restriction on international data transfers<sup>18</sup>.

Due to the foregoing technological advancement, one cannot hope to have the impact of the GDPR fully harmonized all over the EU.

---

<sup>18</sup>Tran (n 16).

### 3.6 Extra-territorial Nature/Reach of the GDPR

If a company is set up or established in the EU, the GDPR will apply. It could be a branch or even a subsidiary; just that there should be effective and real activity via the use of stable arrangements in the EU. However, the GDPR shakes things up and extends the reach of the data protection law to companies based outside of the EU. If you are a company in India and offer goods and services to people in the EU, you are caught in the GDPR net<sup>19</sup>. Additionally, if you monitor the behavior(s) of individuals based in the EU, the GDPR applies to you. It just refers to individuals being tracked online for profiling purposes. So, if you are a business, based in India, but you profile customers are based in the EU and are offered personalized recommendations based on such profiling, then you could be a business falling within the purview of the GDPR. The GDPR applies to you if you track individuals across multiple sites or use applications, etc., to track geo-locations<sup>20</sup>.

Now, you may naturally have concerns regarding what supplying products and services to EU residents entails. Does this mean that if you have a website that can be accessed by people based in the EU, you fall within the ambit of the GDPR? Not really. Several variables come into play when considering whether your actions constitute the provision of goods and services to EU residents. Following is some of the instances which become subject to the GDPR based on "offering goods and services" to individuals in the EU<sup>21</sup>:

1. Using the language that is not even relevant in your own country—for example, if you are an Indian website, but you are using German.
2. If you show prices in Euros whilst Euros is not even used in your home country.

---

<sup>19</sup>Shakila Bu-Pasha, 'Cross-Border Issues under EU Data Protection Law with Regards to Personal Data Protection' (2017) Information and Communications Technology Law 83.

<sup>20</sup>ibid.

<sup>21</sup>Benjamin Greze, 'The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives' (2019) International Data Privacy Law.

3. If the top-level domain name that you are using is that of an EU Member State (e.g., de for Germany).
4. If you are delivering physical goods to an address in, say, Hungary.
5. If your website includes references to Norway-based customers using your products.
6. If a huge percentage of your customers is based in the EU.
7. If you pay for advertisements to be published in a Member State newspaper, whilst your base of operations is the US.

However, just accepting a credit card payment that has an EU billing address does not mean you have to comply with the GDPR. Electronic delivery of goods and services to an individual based in the EU does not automatically mean that company will have to comply with the GDPR. If the internet advertising is seen by individuals in the EU but is not targeted at them<sup>22</sup>, the GDPR does not apply. Just because the telephone numbers provided in the website have international prefixes, the GDPR does not automatically apply to you.

The website may also have to comply with the GDPR if they are dealing with a data controller or processor based in the EU; and also, if they are providing services to a data controller or processor who in turn offers goods and services to individuals in the EU.

To the extent that the extra-territorial provisions of the GDPR apply the website will need to appoint a Representative (it could be a group company) based in EU, in the Member State in which the relevant data subjects are based. One does not have to appoint a representative, however, if the data processing is once-in-a-while in nature, or if such data processing is unlikely to cause risk to individuals, or if there is no large-scale processing of sensitive personal data.

---

<sup>22</sup>Douwe Korff, 'The Territorial (and Extra-Territorial) Application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service' (2019) SSRN Electronic Journal 113.

### 3.7 Lawful Processing

Processing of personal data on lawful grounds is not a new requirement, of course, but it's important to refresh the concept. For Lawful personal data processing, it should comply with all general data protection principles<sup>23</sup>, and it must be backed by at least one of the six grounds for processing. If there is sensitive data processing, then at least one sensitive data processing condition must be met.

### 3.8 GDPR's 6

Here's a quick reckoner on the 6 general data protection principles that were a part of the DPD, as well.

1. Lawfulness, fairness and transparency- Companies must ensure that they process personal data in a manner that is lawful, fair, and transparent<sup>24</sup>.
2. Purpose limitation- Companies must collect personal data for purposes that are specified, explicit, and legitimate<sup>25</sup>, and should not be processed. Further than the identified purposes (unless it is for public interest, or for historical, scientific, and research purposes).
3. Data minimization—Companies must collect/process only as much personal data as is required to fulfill the purpose behind the processing, in that the personal data is “adequate, relevant, and limited” to the identified purpose<sup>26</sup>.
4. Accuracy<sup>27</sup>—Companies must ensure that the personal data that they collect is accurate, and that it is kept up to date. Companies must either rectify or delete inaccurate personal data.

---

<sup>23</sup>Elena Gil González and Paul de Hert, ‘Understanding the Legal Provisions That Allow Processing and Profiling of Personal Data—an Analysis of GDPR Provisions and Principles’ (2019) ERA Forum 321.

<sup>24</sup>ibid.

<sup>25</sup>Himanshu Arora, ‘Grounds for Lawful Processing of Personal Data in GDPR and Personal Data Protection Bill 2018, India (PDPB): Section – VII: Employment Purposes’ (2021) SSRN Electronic Journal 245.

<sup>26</sup>Gil González and de Hert (n 23).

<sup>27</sup>ibid.

5. Retention—Companies must ensure that they keep personal data in an identifiable format only until the time that the identified purpose is served, or in accordance with statutory record retention obligations<sup>28</sup> (exceptions relate to public interest, historical, scientific, or statistical purposes).

6. Integrity and Confidentiality<sup>29</sup>—Companies must ensure that personal data is kept safe and secure, and does not fall prey to unauthorized disclosures, breaches, attacks, etc.

### **3.9 Grounds for the Processing of Personal Data**

Ensuring that grounds for processing of personal data are lawful is not a new requirement. However, with the GDPR coming into effect, it becomes imminent to understand and be able to record these grounds and ensure that they are within the realms of legality. To be considered as processing personal data lawfully, one should have at least one of the following baser grounds covered.

1. Consent—Consent has to be obtained by the “data subject for one or more specific purposes” while processing their personal data.

2. Necessary for the performance of a contract—It is necessary to process data to perform a contract, or where data subject is a party to a contractual obligation, or at data subject's request certain steps need to be taken before entering contract.

3. Legal obligation—The processing is deemed necessary to comply with a legal/statutory requirement that applies to the data controller.

4. Vital interests—Processing is considered essential to defend the vital interests of the data subject or of another natural person.

5. Public functions—Considered required for the performance of a job in the public interest or the exercise of official power vested in the data controller, processing is deemed necessary.

---

<sup>28</sup>Arora (n 25).

<sup>29</sup>Gil González and de Hert (n 23).

6. Legitimate interests—For the purposes of any legitimate interests of the data controller or a third party, processing is deemed necessary except where any such interests are countermanded by the interests of the data subject or the fundamental rights and freedoms accorded to the data subject which require the protection of personal data, especially in instances where the data subject is a child.

There is this popular fallacy that one must obtain individual consent in order to process data lawfully. Truth is that it is not a pre-condition to lawful processing; it is also not a way to circumvent processing activities that would be considered lawful in general. That being said, however, will need consent for other processing activities—for instance, if you intend to send unsought emails or texts a recipient, you will mandatorily require their specific and explicit consent.

In order to bank upon "legitimate interests", you must ensure that you have legitimate business reasons to process personal data. And, you have to ensure that such legitimate interests are not countermanded by the data subject's interests and their rights/freedoms. Furthermore, if you are going to use the legitimate interest's base, you must mandatorily disclose this to the data subject, via a privacy notice (also referred to as fair processing information).

To the extent that you want to further process personal data already obtained for another purpose that was not set forth earlier, you must verify that your new purpose is not completely a mismatch with your older/original purpose of processing. This means that you should compare the purposes, review consequences arising out of the processing (actual and intended), and review safety mechanisms (existing and future) in order to secure the personal data.

Notwithstanding the above, where it comes to processing of special categories of data (personal data relating to race, religion, sex life, health, and political, and genetic and biometric information), you are prohibited from processing such data except in fairly limited circumstances—such circumstances would include where you have obtained the "explicit" consent of the data subject, the

processing, is deemed necessary legally, of where the processing is for reasons of public health and interest.

Processing of data relating to criminal convictions and offences based on a one of the lawful grounds mentioned above must be conducted under auspices of an official authority, or as authorized by EU or a Member State; that provides for adequate and appropriate safeguards.

As per the GDPR, public authorities will no longer be able to use the "legitimate interests" condition and will have to bank upon one of the other conditions (most likely, the public functions condition). This could potentially include not just state entities, but also private entities that provide public service, for example utility companies.

### **3.10 Grounds for the Processing of Sensitive Personal Data**

When it comes to the processing of sensitive personal data, the GDPR has far more stringent restrictions. Although there are more than 6 conditions, these are extremely narrow and far more difficult to base data processing upon. In order to process sensitive personal data, companies must be able to meet at least one of the following 10 conditions<sup>30</sup>:

1. Explicit consent—Sensitive personal data can be processed by organizations if the data subject/individual has given “explicit consent”<sup>31</sup>. However, EU or Member State law may limit the instances in cases where such consent is already available.
2. “Legal obligation related to employment”—Where processing of sensitive personal data is obligatory to fulfill legal/statutory obligations arising out of employment law<sup>32</sup>, or is required under collective agreement.

---

<sup>30</sup>ICO (n 14).

<sup>31</sup>Māris Bomiņš, ‘Consent As A Legal Basis For Processing Of Personal Data’ (2019) Administrative And Criminal Justice 88.

<sup>32</sup>Arora (n 25).

3. Vital interests—Processing of sensitive personal data is to be done to protect vital interests of the data subject or those of another natural person, for example, in case of medical emergency.
4. Not-for-profit bodies—Processing of sensitive personal data is done by non-profit body way of legitimate activity; data remains with the members of that body or other related persons; data is not disclosed outside of that body without data subject's consent.
5. Public information—The processing of those sensitive personal data which data subject themselves has made public.
6. Legal claims—Processing of personal data is required to prove or defend legal claims, or when courts are acting in a judicial capacity.
7. Substantial public interest—When substantial public interest is involved processing of sensitive personal data is required based on EU or Member State law(s).
8. Healthcare—Processing of Sensitive personal data is deemed necessary for healthcare purposes but must be suitably guarded<sup>33</sup>.
9. Public health—Processing of Sensitive personal data is deemed necessary for public health purposes based on EU or Member State law(s).
10. Archive—Processing of sensitive personal data is deemed necessary for archival, scientific, or historical investigation, or statistical<sup>34</sup>, and such processing is based on EU or Member State law(s).

### **3.10.1 Yes, I do / accept – Consent**

---

<sup>33</sup>Mary Kirwan and others, 'What GDPR and the Health Research Regulations (HRRs) Mean for Ireland: "Explicit Consent"—a Legal Analysis' (2021) *Irish Journal of Medical Science* 107.

<sup>34</sup>Olly Jackson, 'GDPR Readiness in the Spotlight' (2017) *International Financial Law Review* 113.



Even though consent is a cornerstone of the GDPR, one cannot rely solely on consent as a ground for processing of personal data. In fact, it would be difficult, foolhardy, and inefficacious to do so.

That being said, though, consent does serve a slew of purposes under the GDPR, it is one of the lawful grounds for processing, even for processing special categories of data<sup>35</sup>. It can also rely on as an exception from the restriction on data export/transfer outside the EEA. One will need it for some of direct marketing activities. However, such consent must be explicit. It cannot be obtained through a course of conduct or be implied.

Note, however, that have to ensure that consent obtained is valid. The GDPR requires that consent be freely given, specific, informed, and unambiguous in nature. How will that be done?

1. Plain language—Whatever form it takes, request for consent must be made in an intelligible and easily accessible form; the language used must be clear, plain and simple. Be careful not to use legalize language.
2. Separate—One must be able to clearly distinguish a request for consent from other matters.
3. Affirmative action—Consent obtained must reflect clear affirmative action (remember that you cannot have pre-ticked boxes; further, silence, lack of a response or inactivity on the part of a data subject cannot be considered as a valid consent).
4. Consent to all purposes<sup>36</sup>—Where processing personal data caters to multiple purposes, one must obtain separate consents for each of those purposes.
5. No detriment/disadvantage—Consent obtained in instances where the individual is unable to exercise genuine free choice or where there is

---

<sup>35</sup>ICO (n 14).

<sup>36</sup>Isabel Maria Lopes and Pedro Oliveira, 'Evaluation of the Implementation of the General Data Protection Regulation in Health Clinics' (2018) *Journal of Information Systems Engineering & Management* 8.

disadvantage in refusing or withdrawing consent, such consent will not be considered valid.

6. No power imbalance—To the extent that there is unbalanced power relationship between the data controller and the individual, consent obtained may not be valid.

7. Not tied to contract—Where consent is considered as a condition to perform a contract (despite consent not being deemed necessary), it will be invalid.

8. Unbundled consent—Do not "bundle" consent. Where there are separate processing activities, the data subject must be able to consent (Note that where consent is revoked, you will have to stop processing personal data, as the consent is not considered valid.

9 Withdrawable—Data subject should be able to withdraw their consent at any given time (it should actually be easy for them to do so). To this effect, you must inform data subject of their right to revoke consent at the time of obtaining consent.

Note: Where consent is revoked, you will have to stop processing personal data, and will have to purge/delete such data, as there is no other legal justification for processing. This basically implies that you may have to significantly invest in processes/systems that would manage the consequences of consent withdrawal.

In instances where consent has been obtained before May 25, 2018<sup>37</sup>, such, consent will be valid but only to the extent that it adheres to the new and more stringent requirements of the GDPR. Where the consent fails to match up to the expectations of the GDPR, a fresh consent may be obtained.

When it comes to direct marketing activities, one can only send direct marketing to someone by e-mail if they have consented to it, or you have an existing relationship with them and fall within the "similar products and services"

---

<sup>37</sup>Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) Information and Communications Technology Law 67.

exemption. Under the GDPR, obtaining consent to e-mail marketing is much harder. There might even be the case that supervisory authorities in Member States may bring in a "double opt-in" model which basically means that once the data subject has provided an initial consent, they must then send them another email which includes a link which they can click upon to validate the initial consent.

### **3.10.2 Consent—Additional Safeguards for Children**

With regard to online services, you will only be able to get consent from a child where it is authorized by a parent. A child is defined as someone below the age of 16, and Member States can reduce this age to 13<sup>38</sup>.

One can rely on the other processing conditions, but practically, it is almost impossible to explain a "legitimate interests" condition whilst processing a child's data. Please note, however, that when providing preventive or counselling services to a child, consent is not required.

The GDPR does not usually apply the "authorization from parent" restriction whilst obtaining consent from a child offline; however, considering how the GDPR treats consent, you'd be better off taking parental authorization<sup>39</sup>.

There are other requirements as well that impact children. Privacy policies that are aimed at children must be extremely clear and simple. There is no way automated decision making and profiling can be directed or applied to children.

Additionally, the right to erase applies robustly and firmly to children. Note that Member State law may have additional restrictions in place with regard to processing of children's personal data<sup>40</sup>.

## **3.11 Rights of Data Subjects**

---

<sup>38</sup>Macenaite and Kosta (n 15).

<sup>39</sup>Marilyn Coleman and Lawrence Ganong, 'Children's Online Privacy Protection Act', *The Social History of the American Family: An Encyclopedia* (2014).

<sup>40</sup>Robert Merrick and Suzanne Ryan, 'Data Privacy Governance in the Age of GDPR' (2019) Risk Management 314.

One of the significant features of the GDPR has been the enhancement, strengthening, and extending of data subjects rights." This includes the following rights of access, right to rectification, right to ensure, right to restrict processing, right to object to processing, right to data portability. The response time for companies has been set forth as a month. There is an additional flexibility of increasing this time period by additional two months where request received are compounded.

In general, as per the GDPR, data subjects have the right to information (via notices), which means that data controllers and processors may be obliged to give data subjects information relating to the following<sup>41</sup>:

1. Contact details of the DPO (that is, if one is appointed);
2. The legal justification or basis behind processing of personal data;
3. Details about international data transfers;
4. Retention periods, or at least the parameters for determining a retention period; the right to object to data processing; the right to data portability; the right to withdraw consent;
5. The right to subject to data processing;
6. The right to data portability;
7. The right to withdraw consent;
8. The right to complain to supervisory authorities;
9. Whether the collection of data is a statutory requirement, or if it is required to enter into a contract;
10. Whether data subjects are required to give data, and if there are consequences of not giving the data;

---

<sup>41</sup>ibid.

11. If there is any automated decision-making, or profiling, the reasons for such processing, and the impact of such processing.

### **3.12 Subject Access Requests**

Data subjects have the right to make a data subject access request (also referred to as DSAR or SAR)—this means that they have the right to seek confirmation from the data controller about the personal data that is being processed about them; they also have the right to ask for a copy of such personal data that the data controller holds about them<sup>42</sup>. By way of this right, data subjects can also ask for information about the sources where their data was collected from, how it is processed, and for what purposes it is being processed for, etc. Companies must provide this information free of any charge/cost to data subjects unless the request is either unfounded, or extremely cumbersome. If the data subject asks for more copies of the personal data, in which case you can charge a small fee. Historically, the exercise of this right has been seen as cumbersome and a fishing expedition (in the legal parlance, you may refer to it as a pre-litigation disclosure tactic).

If a SAR is made electronically (via e-mail), then the information sought should be shared electronically, unless a physical copy has been sought for. In fact, where possible, the data subject should be given secure remote access to their personal data. Companies have a month to respond to a SAR; this period can be extended up to 2 months if the SAR is a complex one, and/or the company is deluged with such requests.

Companies can withhold divulging personal data as a response to a SAR if such disclosure would "adversely affect the rights and freedoms of others". As per the Charter of Fundamental Rights, to be able to conduct business is a right. If we go by that, companies may be able to withhold IP, trade secrets, and other company confidential information by stating that disclosing such information would

---

<sup>42</sup>“Tobias Urban and others, ‘A Study on Subject Data Access in Online Advertising After the GDPR’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (2019).”

adversely impact the right to conduct business<sup>43</sup>. As the dust settles in, we will have a better idea of how the exercise of this right will pan out.

In the past, companies have been able to circumvent and/or dilute DSARs by using the privilege card, or by stating that the requests were cumbersome, etc. However, if one were to look at current regulatory attitude towards enforcement of the GDPR and other data protection laws, it seems unsafe to use such strategies. Furthermore, considering that Member States can introduce exemptions, it is extremely unclear at this point whether regulators will take kindly to companies using such strategies.

Meanwhile here are a few quick tips on how companies can respond to SARs. Once you receive a SAR, you must first try and assess the exact nature of the request (what is it that the data subject wants?). You may also want to consider what personal data you store/process, or that personal data could be lying with third parties, or who will handle such requests within the company and ensure that a response is appropriate, or how the response will be provided for. Also, send an acknowledgment of receipt to the data subject making the request<sup>44</sup>.

A SAR has to be evaluated properly to check that it is valid. A company should run a SAR past the DPO or a data privacy professional to comment upon its validity. If the SAR is found to be invalid, inform the data subject, and give them reasons why. If the request is found to be valid, you must initiate the process of data collection to respond to the request. If you feel that you need further identification proof, please request the data subject to provide such proof.

Once the data collection is initiated, ensure that you have all the personal data of the data subject required to respond adequately to the request—this is where the concept of data mapping and the requirement to maintain records of data processing come in handy. Once all this data is collected, it can be set forth in a

---

<sup>43</sup>Antonio Capodiecici and Luca Mainetti, ‘Business Process Awareness to Support GDPR Compliance’, *ACM International Conference Proceeding Series* (2019).

<sup>44</sup>“Alaa Altorbq, Fredrik Blix and Stina Sorman, ‘Data Subject Rights in the Cloud: A Grounded Study on Data Protection Assurance in the Light of GDPR’, *2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017* (2018).”

spreadsheet or a Word document and should be shared with the DPO<sup>45</sup> or a data privacy expert to review. During the review, if it is found that the company does not have the kind of personal data that has been requested for, a communication should be sent to the data subject to that effect, along with a request that this be acknowledged. Ensure that any extra copies of this data that is shared with DPOs, and others, are deleted<sup>46</sup>. If you have the requisite data, you must respond to the data subject and attach the spreadsheet or the Word document that you have created.

Set forthwith is a simple flowchart that captures the aforementioned steps:

### **3.13 Right to Rectification**

By exercising this right, data subjects can, without undue delay, get inaccurate personal data about themselves rectified<sup>47</sup>. Additionally, depending upon the purposes of processing, they can also have incomplete data completed.

If you have received a request to correct data, you must correct inaccurate data, or you must complete the information that is missing; additionally, you must cease processing until the data is corrected.

### **3.14 Right to Object**

As per the GDPR, data subjects now have more enhanced rights in terms of objecting to data processing. In an instance where the legal justification of processing rests on public interest or where processing is by way of exercising official authority vested in the data controller, the data subject has the right to object to processing. Also, where legitimate business reasons are cited for processing, data subjects have the right to object. This includes having the right

---

<sup>45</sup>Danielle Bauer, '6 Steps to GDPR Implementation' (2018) Risk and Insurance Management Society, Inc.

<sup>46</sup>Aurimas Šidlauskas, 'The Role and Significance of the Data Protection Officer in the Organization' (2021) Socialiniai tyrimai 345.

<sup>47</sup>Michael Hintze, 'Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR' (2018) SSRN Electronic Journal 776.

to object to profiling<sup>48</sup>. So, basically, this means that data subjects can object to processing based on legitimate interests, and to processing in the context of direct marketing, research, statistics, etc. Unlike under the DPD, the data subject no longer has to provide compelling legitimate grounds to object to data processing which was based on legitimate interests. In fact now, it is the data controller/processor that has to prove compelling reasons to process the data despite an objection made, which supersede the rights, freedoms, and interests of the data subject, or they have to prove that such processing is required to establish, exercise, or defend a legal claim<sup>49</sup>.

Note that an individual can object to direct marketing at any time—this is an absolute right, and there are no exceptions.

*Firms providing marketing services to other organizations need to double check whether they have valid consent from people to send marketing emails to them. Generic third-party consent<sup>50</sup> is not enough; companies will be fined if they break the law. ---Sieve Eckersley (Director of Investigations at the UK ICO).*

In an instance where the data subject objects to direct marketing, you must immediately stop sending any marketing material to this individual, and if you are already processing their data, or such data is in your marketing databases, etc., you must immediately stop processing this data for marketing purposes. If you are even profiling for direct marketing purposes, you must immediately stop that.

Note that in terms of the restrictions on direct marketing, the GDPR needs to be read along with the e-privacy Directive (scheduled to become a regulation shortly) which has additional restrictions. If implemented, the new regulation will

---

<sup>48</sup>Michèle Finck and Asia Biega, 'Reviving Purpose Limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems' (2021) SSRN Electronic Journal 675.

<sup>49</sup>Michael Hintze, 'Automated Individual Decisions to Disclose Personal Data: Why GDPR Article 22 Should Not Apply' (2020) SSRN Electronic Journal 28.

<sup>50</sup>Sabina Daniela Axinte, Gabriel Petrică and Ioan Bacivarov, 'GDPR Impact on Company Management and Processed Data' (2018) Quality - Access to Success 341.



replace the existing EU e-privacy and Electronic Communications Directive 2002, which was implemented in the UK in 2003.

### **3.15 Right to Restrict Processing**

Data subjects have the right to get data processing restricted, in the following instances:

1. The data subject challenges the accuracy of personal data and the controller is in the midst of verifying whether the data is in fact accurate;
2. Processing of personal data is unlawful but the data subject exercises the right to restrict rather than ask to be forgotten;
3. The data controller does not need the personal data any longer for the reasons of processing per se, but needs it instead in the context of a legal claim; or
4. The data subject objects to the processing, and it is yet to be determined whether the data controller can continue to process data based on the "legitimate interests" ground.

When this right is exercised, or such a request is made, the data controller should not Process personal data, except with the data subject's consent; or for reasons of establishing, exercising or defending a legal claim; or for reasons of public interest. The data controller can, of course lift the restrictions, the data subject must be informed beforehand.

### **3.16 Right to Data Portability**

This is one of the new features of the GDPR—the right to data portability. What it means is that if a data subject has provided their personal data to you, and you process that data through automated means, and such processing is based on consent or contract, then the data subject can exercise the right to request you to provide them with their personal data in a "structured, commonly used, machine-readable format", and where it is technically possible, to transmit such

data directly to another data controller<sup>51</sup>. Note that although data controllers should use formats (like CSV, XML, and JSON) that facilitate data portability, it is not a mandate that they should develop processing systems that are technically compatible.

### **3.17 Right to Erasure or Right to be Forgotten**

Data subjects can have their personal data erased without undue delay by way of exercising this right. However, this is not an absolute right to the extent that data controllers can continue to process data instances where it is absolutely necessary in relation to the purpose the data was collected for, and where the data controller is not relying on consent as the basis for processing<sup>52</sup>. Additionally, a company can continue to process data for reasons of public interest or in the area, of public health, or where processing is for the reasons of historical research (in this case, the data controller must ensure that appropriate safeguards are place). Bear in mind that the exemption accorded to historical research is one where Member States can derogate.

As stated, this is not an absolute right. It only applies when:

- Data is no longer required.
- Consent has been withdrawn.
- Data subjects object to the use of the data and when their interests outweigh those of the company.
- Data was unlawfully collected/obtained.
- There is a legal obligation to delete the data.
- The data subject was a child when the data was obtained.

---

<sup>51</sup>Paul De Hert and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) *Computer Law and Security Review* 776.

<sup>52</sup>Vincenzo Mangini, Irina Tal and Arghir Nicolae Moldovan, 'An Empirical Study on the Impact of GDPR and Right to Be Forgotten - Organisations and Users Perspective', *ACM International Conference Proceeding Series* (2020).

A challenge which the companies may face whilst responding to a request related to erasing data that is in backup. It is not an easy task to search backfiles/spreadsheets. However, this right applies to data in production, backup archives. Companies must first secure their back-ups to prevent misuse of data.

Note that the GDPR is not applicable to anonymized data. Once the data in backups and archives is identified, these must be deleted. Additionally, where backups are concerned, the company must not make a processing decision affecting individuals<sup>53</sup>. It should mark/flag such data so that it is not misused, and consider additional layers of technology and security, whilst committing to permanent deletion if/when possible.

Once the request is received, the data controller must assess it to ensure that it is a valid request. As soon as possible, the controller should send an acknowledgement of receipt of the request to the data subject. To the extent that the request is deemed to be invalid, the controller should inform the data subject about it along with the reasons for such an assessment. If the request is deemed valid, the controller can ask for further identification, if required. Thereafter, the process of data collection must start. Once the personal data has been collected, all of it must be totally erased. The controller must then share the proof of deleted data with the DPO or with a privacy professional and seek counsel. Once this is approved, it can be shared with the data subject.

If there is no data found, then the data subject must be informed and his acknowledgement must be sought and received.

### **3.18 Automated Decision-making, Processing & Profiling**

---

<sup>53</sup>Marko Milosavljević, Melita Poler and Rok Čeferin, 'In the Name of the Right to Be Forgotten: New Legal and Policy Issues and Practices Regarding Unpublishing Requests in Slovenian Online News Media' (2020) *Digital Journalism* 43.

Data subjects have the right to object to any automated decisions that might have a direct legal or other significant impact on them. Such automated decision making includes those based on automated profiling, as well<sup>54</sup>.

### **3.18.1 Profiling**

The right to object to profiling is not a universal right. This right can be exercised only in certain circumstances. For example, when it comes to direct marketing purposes, data subjects have a broad right to object to any sort of automated profiling. You may ask what constitutes profiling. This could include in scope recruitment e-processes which do not require any human intervention (where job applications and forms are completed via a website or an IT application, for example, SAP Success Factors, and were based on details completed, the application/form can get rejected by the website or the IT app in an automate manner, with no human intervention at all), the automated refusal of an own personal loan application on a bank's website, etc. It also includes instance like using cookies to trace individuals' activities on the worldwide web analyze or predict what they are likely to purchase or using geo-location technology to track movement of individuals.

The GDPR defines profiling as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects relating to that natural person's performance at work, economic situation, health, personal preferences, interests, dependability, location, or movements.<sup>55</sup> Profiling per se, is not prohibited by the GDPR. However, there are restrictions. To the extent that any profiling is backed by a legal ground, and that it complies with the broader data protection principles as enshrined in the GDPR, it is allowed. The GDPR sets forth certain requirements for data controllers in terms of profiling<sup>56</sup>.

---

<sup>54</sup>Adrián Palma Ortigosa, 'Automated Decision-Making in the Gdpr. Algorithms in the Scope of the Data Protection' (2019) *Revista General de Derecho Administrativo* 23.

<sup>55</sup>Gil González and de Hert (n 23).

<sup>56</sup>Chiara Rustici, 'GDPR Profiling and Business Practice' (2018) *Computer Law Review International* 439.

- Controllers shall use appropriate mathematical and statistical processes when undertaking profiling<sup>57</sup>.
- They must implement appropriate technical and organizational measures so that there is as less risk as possible, and in instances any risk or error occurs, these can be rectified<sup>58</sup>.
- Personal data shall be made safe in a way that considers all potential risks to the data subjects' rights, and which prevents any sort of discrimination.

Data subjects can object to profiling which is necessary to perform a public interest task or is part of the official authority that vest in a data controller or is backed by legitimate interest grounds. But, in both these instances, a data controller can dismiss such objection if it can prove that the legitimate interest is compelling enough to overlook the data subject rights and freedoms, or if it can show that such profiling is imperative in terms of any legal claims.

What controllers need to pay special heed to is that they must clearly and explicitly inform data subjects (while first communicating with data subjects), via a privacy notice, that these data subjects have the right to object to profiling<sup>59</sup>. Companies must ensure that this part of the privacy notice is set forth clearly and separately from other parts of the privacy notice so that it catches the eye of data subjects. Additionally, whilst collecting personal data for profiling purposes, companies must inform all data subjects about the facts that the former are collecting data for the purposes of automated decision making and/or profiling. They must state the significance and the anticipated results of such profiling, and also the logic behind such profiling being carried out.

### **3.18.1.1 Decision-making based on Profiling**

---

<sup>57</sup>Gil González and de Hert (n 23).

<sup>58</sup>Frederike Kalthener and Elettra Bietti, 'Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR' (2018) *Journal of Information Rights, Policy and Practice* 112.

<sup>59</sup>Gil González and de Hert (n 23).

We have stated earlier that profiling is permitted (subject to certain limitations and requirements being followed); however data subjects have the right not to be subjected to decision-making which is exclusively based on profiling or a similar automated data processing activity, which decision-making affects them legally and/or significantly. But, again, this is not an absolute right<sup>60</sup>. It is subject to certain exceptions. Companies can make decisions based exclusively on profiling, if the data subjects' explicit consent has been obtained, or if the decision is imperative to enter into a contract, or to perform a contract that is entered into between the company and the data subject; however, the company must ensure that it has implemented appropriate measures to secure data subjects' rights, freedoms, and legitimate interests. Companies can also engage in decision-making based on profiling if it is expressly allowed by EU law or any Member State law that the company subscribes to, and wherein said law sets forth appropriate measures to secure data subjects' rights, freedoms, and legitimate interests. This last exception is not something that companies can rely on, except rarely.

In practice, companies will most likely use consent as the basis for decision-making based on profiling. But whilst companies do so, they must be wary of the extremely stringent consent requirements<sup>61</sup>. They should ensure that all consent obtained is valid. To the extent that companies use the contract exception, they must bear in mind that this exception will apply where there is a pre-contractual relationship between the company and the data subject which sort of mandate the decision in question is.

Apart from ensuring that appropriate measures are in place to secure the data subjects rights, freedoms, and legitimate interests, companies must also inform data subjects adequately about all decision-making based on profiling, and also provide them with the following rights—

---

<sup>60</sup>European Union, Art. 22 GDPR - Automated individual decision-making, including profiling 2018.

<sup>61</sup>Eduardo Ustaran and Victoria Hordern, 'Automated Decision-Making Under the GDPR – A Right for Individuals or A Prohibition for Controllers?' (*Hogan Lovells Chronicle of Data Protection*, 2017).

- (i) right to have human intervention in place;
- (ii) right to express their own point of view;
- (iii) right to an explanation behind the relevant decision; and
- (iv) right to challenge decision taken.

### **3.18.1.2 Privacy Notices or Fair Processing Information**

Data subjects have the right to information. Well, the GDPR requirements for privacy notices must be one of the bigger dichotomies of the Regulation. While on the one hand it requires enterprises to make their privacy statements brief, straightforward, comprehensible, and readily available, on the other hand it forces companies to provide a vast amount of information about how personal data is being handled and other pertinent details.

So, here's how you address this dichotomy.

Consider layering for some weird reason, layering seems to remind you of the tiers of a multi-layered cake. Well, what you can do is that you can set forth in a short summary the purposes behind processing the data and give that to the data subjects, whilst setting out links where data subjects can read the entire notice in detail if they prefer to get details. Let's just admit that most people will not read detailed privacy notices. So, layering helps kills two birds, it sets forth all that a company is going to do with a data subject's personal data, and yet stops short of killing people with information.

For specific instances, consider using additional notices—here's an example. Say, one of your customers wants to do a holiday promotional campaign for its products, and offers attractive discounts to its partners' employees, etc. What you have to do is to provide a link to your employees which takes them to your customer' website/webpage where they might have to enter their personal data (names, email addresses, etc.) in order to avail of the discount. So, here, you can draft a short privacy notice for your employees stating the background and purpose of the promotion, and then informing them that any personal data would

be used by the customer (a third party) in order to facilitate the discounts, etc., and that processing of data would be as per the third party's privacy policy, and that you cannot assume responsibility of the security of personal data given by the employees to the third party on their own accord, and of such data lying in third party' systems.

Avoid legal language and jargon—this is an occupational hazard if lawyers are drafting your privacy notices. However, you must bear in mind that the layman will most likely not be able to make sense of words like "processing", "controller", etc., unless these terms are broken down into plain and simple language and instances that make sense to them. If you are putting up a notice on your website, why not try and use a short video, an animation, or a cartoon about how you process personal data rather than put up a lengthy notice?

### **3.18.1.3 Instances and Exemptions**

As for the timing of privacy notices, these must be provided to data subjects when you collect the personal data from them. However, if you are collecting personal data from a third party, or if you are going to disclose personal data to a third party, you must inform the data subject within a reasonable time-period, but not more than a month after, it was collected. To the extent that this personal data that you obtained from a third party is used to communicate with the data subject themselves, you must inform the data subject when you first communicate with them. And, if personal data is disclosed to a third party, inform data subjects immediately.

However, in certain instances, when you get data from a third party, you may, be required to give notice to data subjects." These instances are set forth here

- (1) if the data subject already has the information;
- (2) if the information to be provided is going to be a cumbersome task (consider where research, or for statistical purposes, etc.);



(3) where obtaining of data from a third party is per EU or Member State law, and there are appropriate security measures in place;

(4) where such information is guarded by reasons of professional secrecy.

When you decide to use obtained personal data for a new purpose, you must provide a privacy notice to data subjects, prior to processing.

### **3.19 Privacy Notices--Form & Content**

In keeping with stricter transparency requirements of the GDPR, privacy notices are an imperative<sup>62</sup>. Companies must provide valid privacy notices to data subjects that inform the latter of the manner in, and the purposes for, which their personal data will be processed. In addition to being short, straightforward, understandable, and readily available (as we saw in Consent), such notifications will also need to fulfil the stricter GDPR criteria (which have been listed in the paragraph below). This essentially necessitates the revision of current privacy notifications, and in certain cases, the creation of new privacy notices.

No matter whether you obtain personal data directly from the data subject, or whether you choose to use a third party for that purpose, you must include the following information on your privacy notice<sup>63</sup>:

- Identification and contact information for the data controller. If the data controller has a representative, add the name and contact information of this person or organisation.
- Name and contact information for the data protection officer of the data controller (DPO)
- The objectives of data processing.
- The legal justification or basis of processing.

---

<sup>62</sup>Kirsten Martin, 'Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online' (2016) *Journal of Legal Studies* 378.

<sup>63</sup>Andrew Denley, Mark Foulsham and Brian Hitchen, 'Privacy Notice(S)', *GDPR – How to Achieve and Maintain Compliance* (2019).

- To the extent that legitimate business interests are the lawful basis of processing, include these interests on the privacy notice.
- To the extent that consent is your lawful basis for processing, include the right of the data subject to withdraw consent.
- Where you collect data via a third party, include the categories of personal data processed.
- Where you outsource or use vendors or other third parties for processing personal data, include the vendor details (recipients of personal data).
- If data is obtained from a third party, and not from the data subject, then include details of the source of such personal data (include the use of a public source too).
- For any actual and/or intended transfer of data outside of the EU include details of such transfer, and of the safeguards used.
- Retention period of personal data, and the criteria used to calculate the retention period (statutory, tax purposes, others).
- Includes details about data subjects' rights. This should also have details about the right to complain to a supervisory authority.
- To the extent that you carry out any automated decision making (including profiling), include details.

### **3.20 Accountability**

Right when you were thinking that it is enough that you comply with the six (6) data protection principles and with the processing conditions, it seems like this is

not going to be enough. The GDPR requires that you are able to show that you are complying<sup>64</sup>.

The GDPR introduces concepts of accountability, privacy by design and by default, data privacy impact assessments, etc. These will enable supervisory authorities to dig deep into a company's processes in order to verify whether they are actually complying with the requirements. What it means for companies is that they cannot anymore think of privacy as a mere sidenote or a reference point; privacy needs to be embedded into a company's systems and processes—they need to be breathing and living privacy.

### **3.21 Data Mapping**

You must have heard of the gold rush in America (specifically in and around, Colorado) way back in the 1850s and thereafter. Scenes of "Mackenna's Gold" (starring Gregory Peck and Omar Sharif) play in your head—early prospectors, explorers, etc., "mapping" their way to Colorado, to the Grand Canyon, drawn in by the tales of rivers flowing with gold. Somehow, when you look at how the concept of personal data has evolved over the last few decades and looking at the role that smart use of personal data plays in boosting business profitability, you could think of personal data as the new gold.

Just like the physical map played an important part during the "gold rush" plays, in modern times, in order to use personal data smartly, companies need to invest in data mapping which is basically all about recognizing, locating, deciphering, and charting out the personal data flows within the company<sup>65</sup>.

What exactly is data mapping, you might ask. If we are still using "gold rush" metaphors, think of Gregory Peck and Omar Sharif (rather, their respective characters) trying to one-up each other in their search for gold, fighting over torn map in order to chart the area around the Grand Canyon and the Colorado river,

---

<sup>64</sup>European Commission (n 12).

<sup>65</sup>Alexia Dini Kounoudes and Georgia M Kapitsaki, 'A Mapping of IoT User-Centric Privacy Preserving Approaches to the GDPR' (2020) Internet of Things.

decoding what the map states about following the rising sun's shadow all that jazz. Sounds complicated? Well, it isn't, not really<sup>66</sup>. Thankfully, one does not need to follow the sun's shadow to anywhere in this case. However, one does need to chart out the 5Ws of personal data, as they are popularly referred to. Those would be—WHO, WHERE, WHAT, WHEN, AND WHY. Let's try simplify these, shall we?

**WHO**—Who are the data subjects? Who are the data controllers? Who are the data processors?

**WHERE**—Where is the data located? Transferred to locations outside the EU.

**WHAT**—What personal data is being collected? What's the purpose behind collecting and processing such personal data?

**WHEN**—How long will the personal data be retained? When will it be deleted, destroyed?

**WHY**—Why do you need to process the data? Why do you need to keep this data after the purpose has been served?

Data mapping is not a GDPR requirement per se; however, it does help the organization is complying with its various other GDPR, and other applicable personal data protection statutory/regulatory obligations. Additionally, it can assist in using personal data in a smart manner in order to derive operational benefits. From a GDPR compliance perspective, data mapping helps data controllers and processors to maintain detailed records of their data processing activities, to be made available to Supervisory Authorities on request. It also caters to the accountability requirement of the GDPR. Furthermore, it helps in meeting the Privacy by Design and by Default requirements<sup>67</sup>.

---

<sup>66</sup>Ellen Poplavska and others, 'From Prescription to Description: Mapping the GDPR to a Privacy Policy Corpus Annotation Scheme', *Frontiers in Artificial Intelligence and Applications* (2020).

<sup>67</sup>Ke and Sudhir (n 19).

Apart from helping a company meet statutory obligations, data mapping assists in a myriad of other ways.

- By way of identifying business processes and IT systems that deal with personal data, and by conducting adequate privacy risk assessments impact assessments of such processes and systems, companies are to figure out if system efficiencies can be improved, and data flows can be managed more efficiently.
- Companies can also determine how data can be used in smarter ways, whilst adhering to controls and limitations, as prescribed by the law.
- Companies, while mapping data, are able to assess the risks of data breach (via appropriate risk and impact assessments), and are, therefore, able to foresee unpleasant situations so that they can take appropriate a risk mitigation measures. In this way, a company can mitigate both reputational as well as financial loss.
- A data map can help a company respond effectively to data subjects' requests. In a pre-litigation or litigation scenario, it assists in responding to discovery requests, and, therefore, minimizes related costs.
- It helps comply with various other statutory record retention requirements, etc.

### **3.22 Maintaining Data Protection Registers**

In keeping with the data mapping activity described previously, the companies will need to keep records of processing. Although the GDPR does do away with the need to notify local supervisory authorities about data processing activities, companies still have the responsibility to maintain detailed records of all data processing activities (and be able to showcase them to the supervisory authority if they come visiting).

In terms of the content of these registers, Member States set forth varying obligations—in the UK, it would be sufficient to have brief summaries while, in France, a company might be required to keep extremely detailed information.

Good news is that small companies (employing less than 250 employees) need not do this unless they engage in high-risk processing, frequent processing, or processing of data that is sensitive.

Most organizations are finding it tough to wrap their heads around this requirement. We saw a passing reference to it in the Data Mapping section earlier. From the periphery, it does appear quite tough and onerous. These records have to be maintained so that they can be provided to the supervisory authority on request. When you think of legacy data, this requirement seems particularly cumbersome, and it probably is. To configure old systems to maintain records of all personal data within an organization is quite exacting; however, the great news is that there are several new and innovative technical solutions available in the market currently that can help organizations in building and maintaining their data maps (or, data inventories), and data protection registers (DPRs) or the records.

### **3.23 Data Controller—Data Processing Register Obligations**

**Data controllers** will be required to maintain DPRs which must include the following information<sup>68</sup>:

- The name and contact information of the controller, the names and contact information of any joint controllers (where applicable), and the names and contact information of the controller's representatives or data protection officers.
- The reasons for data processing.

---

<sup>68</sup>Shakila Bu-Pasha, The Controller's Role in Determining High Risk and Data Protection Impact Assessment (DPIA) in Developing "Digital Smart City" (2020) Information and Communications Technology Law 771.

- Descriptions of the types of data subjects and personally identifiable information.
- Descriptions of types of receivers of personal data (including third parties in foreign countries and/or international organisations).
- Details of personal data transfers to foreign nations.
- “Retention periods” for different categories of personal data.
- General description of the security measures in place. companies would be required to answer the following questions:

1. What personal data companies have got/collected? (Name, telephone number, address, date of birth, etc.)
2. Why do the companies have the personal data? (Legal basis for processing)
3. Where or with whom do companies share the personal data (Internally? Externally? or Both?)
4. How do you share the personal data in a protected manner? (Data transfers/safe data transfer mechanisms)
5. For how long is the personal data retained? (Retention policies)
6. When and how do companies delete/destroy data? (Consider both hard and electronic copies)
7. How do companies ensure security of the personal data? How do companies ensure that the security controls in place are effective?

### **3.24 Data Processors—Data Processing Registers Obligations**

**Data processors** would be required to maintain the following information<sup>69</sup>:

---

<sup>69</sup>Yordanka Ivanova, ‘Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World’ (2020) SSRN Electronic Journal 109.

1. Name and contact details of the processor, any representatives (where applicable), and the name and contact of the appointed DPO;
2. The name and contact details of the data controller, their representatives (where applicable), and their DPOs.
3. The categories of data processing that the processor carries out for the controller.
4. Details of any international transfer of personal data (outside of the EU)
5. Details of security controls in place to keep the data safe and secure.

### **3.25 Data Privacy Impact Assessments**

The GDPR requires that companies that engage in any "high risk" projects and/or processing activities must conduct data privacy impact assessments (DPIAs). In any case, by way of the previous DPD, several companies were conducting such PTAs for technology that they used for processing of personal data. Here are a few things that you must consider in terms of conducting DPIAs.

First and foremost, consider whether the processing can be seen as "high risk." The GDPR provides some guidance on this point and sets forth some examples such as artificial intelligence, smart technologies (including wearables), credit checks, social media networks, workplace access systems/ identity verification.

DNA testing etc. Where a DPIA is required, companies must seek advice from the DPO or a privacy professional. In instances, where a DPIA is conducted, and it seems that the remediation measures in place are not sufficient in relation to the risks, then companies must consult the local supervisory authority and seek advice. Please note that any such consultation would require time – supervisory



authorities have upto 14 weeks to consider your application for a consultation and can even extend this time<sup>70</sup>.

### **3.26 Data Protection Officers**

We had mentioned "beat cops" before. Depending upon the data processing that you carry out, you may be obliged to appoint a beat cop, or a data protection officer (DPO). Cannot terminate the services of your DPO for doing their job, and your DPO must be reporting to the highest-management levels in the company.

The DPO is a very important element of the "accountability" framework that we discussed before. DPOs are mandated by Member States like Germany<sup>71</sup>.

If required to do so by the legislation of your Member State, you must designate a DPO if you are a public entity (except for courts acting in their judicial capacity), if your core processing activities are about large scale, regular and systematic monitoring of data subjects, or if you are processing sensitive data on a large scale (such data includes information about criminal offenses).

The obligation to appoint a beat cop (or DPO) rests on both data controllers and processors. Even if you are not mandated to do so, it is just a good idea to voluntarily appoint a DPO, as they add significant value to your privacy compliance program and are also your representative before a supervisory authority. However, note that even with a voluntary appointment, all other GDPR provisions with regard to a DPO will kick in (including shelter from dismissal). To avoid this, be careful of the title you offer to the DPO, and the job description and scope of their activities.

A group of companies may want to have a single DPO, but they must ensure that this individual is easily accessible to all units of the group, and that they are a

---

<sup>70</sup>Dimitra Georgiou and Costas Lambrinouidakis, 'Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations' (2021) Future Internet9.

<sup>71</sup>Minjung Park, Sangmi Chai and Myoungjun Lee, 'A Study on the Establishment of Data Protection Officer(DPO) Position under GDPR Enactment' (2018) The Journal of Korean Institute of Communications and Information Sciences 117.

subject matter expert in all matters related to data privacy. However, this might be a problem if the DPO does not speak the language of a particular jurisdiction where there are several data subjects, or if the DPO does not reside in, or is not familiar with the requirements of a particular Member State where one of the group companies might operate in. In such cases, you may want to have a group DPO, and then appoint several other data privacy experts/leaders in other group entities and jurisdictions that report to this group DPO.

### **3.27 Roles & Responsibilities and Qualifications of a DPO**

The basic responsibilities of a DPO are to monitor and supervise whether you are complying with the GDPR, to inform and advise you, and to liaise with supervisory authorities. They should be able to operate independently and must have access to all resources that they need to comply with the GDPR. A DPO can also have other roles within the company if there is no conflict of interest—for example, they cannot be a CISO, or an HR head, or part of the Compliance team, as that would mean marking their own homework<sup>72</sup>.

There is no mandatory qualification that a DPO must have—it is good to have relevant certifications, like CIPP<sup>73</sup>, etc., but the lack of such certifications is not a deal-breaker. If the DPO has subject matter expertise when it comes to data Privacy regulations, implementation, and practice, it is good enough. The WP29 has defined certain minimum requirements when it comes to acumen of a DPO<sup>74</sup>:

- The DPO is expected to be an expert in building and implementing effective data privacy programs.

---

<sup>72</sup>ibid.

<sup>73</sup>Timothy Banks, ‘GDPR Matchup: Canada’s Personal Information Protection and Electronic Documents Act’ (2017) The International Association of Privacy Professionals.

<sup>74</sup>Marija Boban, ‘Protection of Personal Data and Public and Private Sector Provisions in the Implementation of the General Eu Directive on Personal Data (GDPR)’ (2018) 27th International Scientific Conference on Economic and Social Development.

- The DPOs need not be lawyers, but they should possess in-depth knowledge of applicable data privacy legislation, and how to put statutory requirements into practice.
- Certifications like CIPP, CIPM<sup>75</sup>, are not mandatory, but good to have.
- The DPO should possess deep knowledge of IT security, infrastructures etc.
- To top it all, the DPO must be able to demonstrate the highest levels of integrity and ethics and be able to thus comply with the GDPR.

### **3.28 Privacy by Design and by Default**

To start with, Privacy by Design and by Default requirements of the GDPR apply only to data controllers, and not to data processors. Although the concepts of Privacy by Design and by Default have been thrown around in conversations, and have been discussed in boardrooms, and have been a mainstay of data privacy discussions all around the world, these requirements have rarely been legislated except for countries such as Canada and Australia. That is, until now. The GDPR requires companies to now implement this approach, especially while creating databases, systems, technologies, infrastructure, etc. What it means is that companies will now have to focus on privacy upfront (and not treat it as a footnote) and right at the beginning and embed privacy into the very architecture of its processes and systems. Data protection cannot be mere lip-service anymore.

Whenever a company is undertaking a new activity involving processing of personal data or is implementing a modified or new system that processes personal data, the GDPR requires the company to consider the approach of

---

<sup>75</sup>Banks (n 73).

Privacy by Design<sup>76</sup>. The company must, thus, take appropriate steps to ensure compliance with data privacy principles, and safeguard their processing whilst meeting data privacy requirements and protecting data subjects' rights, both while deciding upon the means of processing and while the processing is happening. This would include considering the idea of limiting the processing of data and/or data minimization. While considering Privacy by Design, the company must look at the following: kind of technology used (should be state of the art preferably), cost of implementation of such technology, the nature, scope, purposes, etc. of the processing activity, risks to data subjects, etc.

The GDPR also requires data controllers to implement Privacy by Default—it is a follow-up to Privacy by Design, and it ensures that personal data is not, by default, made available or accessible to multiple and/or unauthorized users. For example, profiles on a website should not, by default, be set up as "public". It means that only personal data which is identified as being absolutely necessary for specific processing purposes is processed, by default.

### **3.29 International Data Transfers**

Transfer of personal data outside of the EU is prohibited under the GDPR regime, unless certain conditions are fulfilled. There are some minor exemptions to this. Although the broader provisions remain the same as in the DPD, there are some significant changes. For example, consent for data transfer must be explicit, and is subject to several other limitations<sup>77</sup>. Unlike before, the use of Model Contract Clauses does not need authorization by a supervisory authority; however, they may still want to be informed about the use of these clauses. Further, the Binding Corporate Rules now have statutory backing behind them<sup>78</sup>. There is also a push for data controllers and data processors to follow codes of conduct or have certifications in place to be considered adequately safe in terms

---

<sup>76</sup>Harald Gjermundrød, Ioanna Dionysiou and Kyriakos Costa, 'Privacytracker: A Privacy-by-Design GDPR-Compliant Framework with Verifiable Data Traceability Controls', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (2016).

<sup>77</sup>Tran (n 21).

<sup>78</sup>Zuzanna Gulczyńska, 'A Certain Standard of Protection for International Transfers of Personal Data under the GDPR' (2021) *International Data Privacy Law* 11.

of data transfers. Transfers can be prohibited due to public interest or under EU or Member State law—the prohibition does not apply to transfer to adequately safe jurisdictions but applies to transfers made based on Model Contract Clauses.

One of the biggest challenges regarding cross-border transfers arises in the instance of onward transfers of data. The extension of data transfer restrictions to onward transfers has rendered things to be quite complicated. How does one decide liability if there is an onward transfer that breaches the GDPR? Will the initial exporter be liable considering that in most cases the importer may not be subject to the GDPR? But then that would be unfair as the initial exporter has limited control over the importer (especially where the importer acts as a controller)<sup>79</sup>.

There is a minor exemption in place for cross-border transfers<sup>80</sup>, especially in instances where an employee travels abroad and carries their laptop with them, or where an employee emails a person who happens to be outside of the EU. The minor exemption applies where no other basis for cross-border transfer can be used, where the transfer is not repetitive in nature, where only very few data subjects are impacted, where there is a compelling business interest that does not supersede the rights and interests of data subjects, where risks have been assessed and appropriate safety controls have been put in place, and where data subjects and supervisory authorities have been notified about the transfer<sup>81</sup>.

Keeping the above in mind, it seems quite implausible that the minor transfer exemption will come into play. It is not feasible that a company will notify data subjects each time an employee decides to take a vacation abroad and takes his laptop with him, or to notify supervisory authorities if an employee sends an email to someone sitting in a foreign country.

---

<sup>79</sup>Martina Mantovani, ‘Contractual Obligations as a Tool for International Transfers of Personal Data under the GDPR’ (2020) SSRN Electronic Journal 32.

<sup>80</sup>Danny S Guaman, Jose M Del Alamo and Julio C Caiza, ‘GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps’ (2021) IEEE Access 203.

<sup>81</sup>Itziar Sobrino García, ‘The Adequacy Decisions in Cross-Border Data Transfers. The Case of Data Flow between the European Union and the United States’ (2021) Revista de Derecho Comunitario Europeo 21.

Also, what does a data controller do if faced with requests for personal information coming from foreign regulators? How do they balance data protection obligations with the risk of being sanctioned by foreign regulators and/or courts? The GDPR states that for a national/local court to consider any foreign disclosure request, such request has to be made under an appropriate treaty. Also, again, cross-border transfer on account of foreign disclosure requests is allowed where there is public interest at play, or where it is on account of legal claims.

### **3.30 Data Security Breach Notification**

Data controllers are obligated to notify the supervisory authority in case of a personal data breach, and in some instances, may also be required to inform data subjects<sup>82</sup>. Data breach notification rules are not a new concept—they have been around for years specifically for telecom providers globally, and in almost states across all sectors in the US.

A personal data breach happens when a security breach leads to the unintentional or illegal destruction, loss, modification, disclosure, or access to personal data.<sup>83</sup> The GDPR applies only to actual, and not to potential, breaches.

The first thing to do when a breach occurs is to assess if it is going to pose a risk to data subjects. If there is a finding of no risk, or very minor risk, then you may not need to notify the supervisory authority. But you will still have to maintain records of the data breach.

If there is a finding of risk to data subjects, you must notify the supervisory authority as soon as possible, and definitely within 72 hours from when you know of the breach. This notification must include everything that you know about the breach (this 'information can be provided in stages if not available immediately). If a breach poses high risk to individuals, then the affected data

---

<sup>82</sup>Maria Karyda and Lilian Mitrou, 'Data Breach Notification: Issues and Challenges for Security Management' (2016) Mediterranean Conference on Information Systems (MCIS) 9.

<sup>83</sup>Chlotia Garrison and Clovia Hamilton, 'A Comparative Analysis of the EU GDPR to the US's Breach Notifications' (2019) Information and Communications Technology Law 67.

subjects need to be informed as well. Such notification must be made immediately and must be detailed. If communicating directly with data subjects proves to be cumbersome, then companies can use alternative methods such as newspaper releases, etc. Note that if the personal data that is breached was encrypted or if there were appropriate technical and physical safety mechanisms/controls in place, then a breach will not be considered high risk. If there is no high risk, then no further notification is required, and you can close the process after all internal action plans have been completed.

### **3.31 Data Processor Obligations**

Under the older DPD, data processors had the safety net of the data controllers. However, this safety net has quite literally been taken away under the GDPR. The GDPR, in fact, imposes data protection requirements directly on data processors, and will hold them directly liable for non-adherence<sup>84</sup>.

Here's a bird's eye view of the main obligations that have been imposed directly upon data processors. These obligations have been articulated in Article 28 of the GDPR.

- Implementing suitable technological and organisational safeguards to protect personal information.
- Maintaining detailed records of all data processing activities.
- Appointing a data protection officer, as required in certain instances of data processing, and appointing a representative that is in the EU in a situation where the processor is based/located outside of the EU.
- Adhering to cross-border transfer requirements/mechanisms.
- Informing data controllers of data privacy breaches.

---

<sup>84</sup>Jenna Lindqvist, 'New Challenges to Personal Data Processing Agreements: Is the GDPR Fit to Deal with Contract, Accountability and Liability in a World of the Internet of Things?' (2018) *International Journal of Law and Information Technology* 211.

I have made a deeper foray into these data processor obligations in the following sections. In this section we will take a cursory look at how these obligations will impact data processors, data processing agreements, relationship between data controllers and data processors, etc.

The definitions of data controllers and data processors remain largely the same under the DPD and the GDPR. A processor is a natural or legal person, public authority, agency, or other entity that processes personal data on behalf of a controller. A controller has been defined as the natural or legal person, public authority, agency, or other body that alone or jointly with others determines the purposes and means of processing personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for designating the controller) may be designated by those laws.

One major aspect that has been brought to the forefront by the GDPR is the level of enforcement against data processors. Now, more than ever, we will see how Supervisory Authorities (SAs) will have direct enforcement powers against data processors. SAs can now, whilst executing their investigating powers, directly seek information from data processors, or ask them for access into the latter's premises or to the personal data. SAs can also put to use their corrective powers, issue cautionary notices and/or admonition, or just demand that data processors comply with the GDPR. And let's not forget the significant administrative fines that could be levied (€20 million, or up to 4% of the annual turnover)<sup>85</sup> (details are provided in the section on Enforcement and Sanctions).

While earlier, the DPD was not extremely comprehensive about the entire process of deciding upon processors (and, sub-processors), the GDPR ups the game quite a bit, and is extremely prescriptive about this topic.

### **3.32 Choosing the right processor**

---

<sup>85</sup>Paul Voigt and Axel von dem Bussche, 'Enforcement and Fines Under the GDPR', *The EU General Data Protection Regulation (GDPR)* (2017).



Whilst choosing a data processor, the data controller should consider someone that can give sufficient guarantees about the implementation of adequate technical and organizational measures per Article 32 of the GDPR<sup>86</sup>. This can be quite a challenge for data controllers—the due diligence which is required, and, therefore, if data processors adhere to an approved code of conduct' or have a certification (such as ISO 27001, ISO 27002, ISO 18028, SSAE 16 etc.)<sup>87</sup> in place, such data processors will score brownie points when it comes to controllers choosing data processors.

### **3.33 Having a Data Processing Agreement (DPA) in place**

Once a data processor is selected, the controller and the processor should enter into a DPA which sets forth the subject matter of data processing, the nature, the purposes, duration, data subject categories, personal data types, rights and obligations of the data controller, etc.

What a DPA does primarily is that it obligates data processors to do the following:

1. Process personal data only as per the instructions of the data controller (such instructions shall be documented). Where such processing relates to data transfers outside of the EU and is required by the Union or the Member State law where the data processor is, the data processor shall inform the data controller of any legal requirement, unless it is prohibited to do so by way of public interest<sup>88</sup>.
2. Ensure that its employees, contractors, representatives, etc., that are processing the data or are authorized to process the data have signed on to appropriate data protection and confidentiality obligations (this basically entails having signed NDAs in place).

---

<sup>86</sup>Catherine Barrett, 'Emerging Trends From The First Year Of EU GDPR Enforcement' (2020)*The SciTech Lawyer*.

<sup>87</sup>Eric Lachaud, 'ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification' (2020) *European Data Protection Law Review* 546.

<sup>88</sup>Fabian Simon Frielitz and others, 'The Contract Data Processing Contract (DP Contract): Relevance and Practical Significance for Diabetology' (2020) *Diabetologie und Stoffwechsel* 77.

3. Take adequate and applicable security measures to protect the personal data.
4. Take prior consent from the data controller before engaging sub-processors, and have such sub-processors sign on to similar DPAs<sup>89</sup>.
5. Help data controllers in responding to data subjects' requests.
6. Help data controllers in complying with obligations relating to data security, data breach notifications, privacy impact assessments, etc.
7. Ensure that personal data is either deleted, shredded, and/or returned, depending on what the data controller wants, once the project or the engagement is over, and delete any existing copies, unless there is a legal requirement to retain such data.
8. Cooperate with the data controller in providing whatever information is required to demonstrate compliance with data processor obligations, and assist data controller in audits, inspections conducted by the controller or its representatives.

### **3.34 Sub-processing**

If the data processor chooses to subcontract, then the following should be kept in mind<sup>90</sup>:

1. When engaging a subcontractor or a sub-processor, the data processor must obtain prior consent from the data controller (such consent has to be written or documented and can be general or specific). If a general consent has been obtained, then in every instance where the data processor wants to change or add sub-processors, it must inform the data controller, and check whether there is an objection.

---

<sup>89</sup>ibid.

<sup>90</sup>Cyber GRX, '6 Security Controls You Need For General Data Protection Regulation (GDPR)' (*Product Resources*, 2018).

2. When subcontracting, the data processor must pass on all obligations imposed by the data controller to the sub-processor by way of a DPA.

3. The data processor is liable to the data controller for the performance of the sub-processor's obligations in the event of failure on the part of the sub-processor to perform its obligations.

### **3.35 Increased liability**

In the current GDPR regime, data controllers continue to remain liable for any damage that is caused by processing which is non-compliant with the GDPR. Data processors, on the other hand, are only liable for damage caused by any processing to the extent that they fail to comply with data processing obligations under the GDPR, or, if they act outside of the ambit of the data controller's instructions. However, this is a significant shift from the DPD where data processors were not directly liable to data subjects for damage caused by processing.

For both, data controllers and data processors, there is exemption from liability if they can demonstrate they did not cause the alleged damage. Additionally, they can be held jointly liable for damage caused by any processing that they do together.

### **3.36 The Security Principle**

As per the GDPR, data controllers and data processors shall process data in a safe and secure manner whilst using "appropriate technical and organizational measures"<sup>91</sup>. This, basically, implies that they must consider aspects like a privacy risk analysis, policies and processes, and physical and technical measures to ensure safety of processing of data. Controllers must ensure that their processors also take into account security of personal data (by way of data processing agreements, etc.). Security measures, whilst taking into account state

---

<sup>91</sup>Antoni Gobeo, Connor Fowler and William J Buchanan, '5 Data Protection by Design and Default', *GDPR and Cyber Security for Business Information Systems* (2020).

of the art, and the cost aspects, must also be associated closely with the types of processing and the underlying risks. Controllers and processors should consider options such as pseudonymization and anonymization<sup>92</sup>. All measures taken should ensure "confidentiality, integrity, and availability"<sup>93</sup> of systems and services that include processing of personal data. Aspects such as data recovery, disaster recovery, etc., have to be taken care of. Controllers and processors should also consider aspects such as vulnerability assessments, penetration testing, privacy risk assessments, etc.

### **3.37 The GDPR Sanctions Regime**

When it comes to punishments, the GDPR provides consequences that leave everyone stunned. Under the GDPR, supervisory agencies may impose penalties of up to €20 million or 4% of the prior fiscal year's global annual revenue, whichever is greater. And if you believed they would stop there, you are incorrect. The government has the authority to give warnings and may audit you at any moment. They may even temporarily halt your processing operations. Data subjects may individually sue you for damages recompense (material damage, as well as for the distress caused). You may also be sued by non-profit organisations representing data subjects.

The larger fine of €20 million or 4% of the total worldwide annual turnover of a business in the preceding financial year applies to non-compliance to provisions such as failure to comply with the 6 general data protection principles, or for carrying out processing without meeting at least one processing condition. The lesser penalty of 2% of a company's annual turnover or €10 million applies to non-compliance like failing to notify a data breach, or failure to put together an adequate contract with a data processor.

---

<sup>92</sup>Peter Štarchoň and Tomáš Pikulík, 'GDPR Principles in Data Protection Encourage Pseudonymization through Most Popular and Full-Personalized Devices - Mobile Phones', *Procedia Computer Science* (2019).

<sup>93</sup>Jan Zibuschka and others, 'Anonymization Is Dead - Long Live Privacy', *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft für Informatik (GI)* (2019).

While determining appropriate sanctions for non-compliance, the supervisory authorities are likely to look at several things, including the nature and seriousness of non-compliance, whether there was negligence or malefic intent, what steps were taken to remediate the breach, any financial benefits derived from the breach, whether the company cooperated with the supervisory authority in any investigations, audits, etc.

### **3.38 Data Ownership**

#### **3.38.1 What do we mean by Data Ownership?**

The rapid expansion of the digital world has led to questions being raised regarding the ownership of data—who "owns" data? When I provide my data to a third party, am I handing over "ownership" of that data?<sup>94</sup> This also brings into play an interesting question on the intellectual property rights associated with the data—who is the copyright holder of the data?<sup>95</sup>

Data ownership means owning and having legal rights and complete control over data—whether as a single piece or as a set of elements. It is interesting to note that the GDPR, which is focused on the protection of an individual's rights to their personal data, does not make any reference to the term "data ownership". An individual whose data is being processed, is not referred to as a "data owner". Instead, terms such as "data subject" and "data controller"<sup>96</sup> are used. India's draft legislation on privacy also does not contain any references to the terms "data owner" or "data ownership"<sup>97</sup> and instead uses terms such as "data

---

<sup>94</sup>Christian Janßen, 'Towards a System for Data Transparency to Support Data Subjects', *Lecture Notes in Business Information Processing* (2019).

<sup>95</sup>Udo Milkau, 'The GDPR: Halfway between Consumer Protection and Data Ownership Rights.' [2018] *Journal of Digital Banking*.

<sup>96</sup>Ivanova (n 96).

<sup>97</sup>Milkau (n 136).

principal" and "data fiduciary"<sup>98</sup>. So, the question that can then be asked is does the law not safeguard my interests as a data owner?<sup>99</sup>

### **3.39 Legal Data Ownership**

In this context, it is interesting to read the provision of the GDPR which deals with data portability and the right to be forgotten. Under Article 20 of the GDPR<sup>100</sup>, the data subject has the "right to receive personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, and machine-readable format and to transmit those data to another controller without hindrance from the controller to which the personal data were provided, where the processing is based on consent and has been carried out by automated means.

Individuals have the right to have their personal information directly communicated from one controller to another (if technically feasible). Coupled with the GDPR's right of erasure and right to be forgotten, this essentially means that an EU citizen can move his personal data from one supplier of services (such as platforms hosting playlists, social networks, etc.) to another and request the original supplier to delete (subject to legal requirements) all references to his / her personal data. In fact, the individual is now, for the very first time, the proprietor of his or her own personal information.

This shift in ownership of personal data could have far-reaching repercussions with leverage on the side of the person owning data. I could seek discounts with my grocery store in exchange for retaining my personal data with them; threaten to shift my personal data if I have had a terrible interaction with a company; participate in a social media program boycotting certain organizations for their

---

<sup>98</sup>“Julia M Puaschunder, ‘Data Fiduciary in Order to Alleviate Principal-Agent Problems in the Artificial Big Data Age’ [2019] SSRN Electronic Journal.”

<sup>99</sup>Julia M Puaschunder, ‘Data Fiduciary in Order to Alleviate Principal–Agent Problems in the Artificial Big Data Age’, *Information for Efficient Decision Making* (2020).

<sup>100</sup>“Ralph O’Brien, ‘Privacy and Security: The New European Data Protection Regulation and It’s Data Breach Notification Requirements’ [2016] Business Information Review.”

perceived abuses.' Since predictions are that data is the next liquid gold, I could sell my data to the highest bidder as well.

### **3.40 Legal Data Ownership vs. Assignment of Data Ownership**

What we have dealt with above is the legal ownership of personal data. However, who 'owns' the data within an organization to whom the data subject has entrusted his / her personal data, is a question that also needs answering. Take for instance, the banking sector. An individual may have submitted her personal data for the purpose of opening a bank account. But there are other departments as well—housing finance, car financing, investment advisory etc. So, who then takes stewardship of that personal data?

This brings in the concept of 'enterprise data. According to The Data Governance Institute, enterprise data doesn't "belong" to individuals. It is an asset that belongs to the enterprise which needs to be managed. Assignment of data ownership within an organization becomes significant—whether it is for the purpose of accountability, defining retention and deletion policies, creating trusted data or eliminating redundancies. An organization needs to determine and assign an 'owner' within the organization who will make final decisions with respect to the data. It could be a single owner or multiple (i.e., different owners for financial, product and customer data). However, not assigning data ownership within the organization could lead to different departments taking different decisions with respect to the data and leading to a frustrating customer experience (let's not forget the customer's right to data portability and erasure).

## **3.41 COMPARITIVE LAW ANALYSIS OF DIFFERENT LEGISLATIONS**

### **3.41.1 India**

Due to the mechanical inefficiency of the provisions of Information Technology Act, 2000, the government authorities were compelled to ponder the rising concerns of privacy of individual data, which is now considered a matter of national security. The Indian government's endeavor

to regulate the collection and use of personal data dates back to 2012 when the committee led by Justice A.P. Shah<sup>101</sup> released its report on privacy. To fully comprehend the privacy concerns and to come up with a viable Bill to address all these issues, the Government of India formulated a data protection committee under Justice B.N Srikrishna. The committee filed its report, commonly known as the Srikrishna Committee Report<sup>102</sup> on July 28, 2018. Thereafter, the draft Personal Data Protection Bill, 2018 was tabled in the parliament. Afterwards, a revised Personal Data Protection Bill, 2019 (hereinafter referred to as PDP Bill, 2019) was introduced by the “Ministry of Electronics and Information Technology” in the “seventeenth Lok Sabha” on December 11, 2019. The committee was constituted by the Ministry of Electronics & Information Technology, Government of India. The Bill was withdrawn in July 2022. The Bill was broadly based on the framework of the General Data Protection Regulation of the European Union and on the principles of the landmark judgement of the Hon’ble Supreme Court of India in justice K.S. Puttaswamy (Retd.) & Anr. V Union of India & Ors.<sup>103</sup> The Bill if implemented would have come in suppression of Section 43A of the Information Technology Act, 2000<sup>104</sup> (The IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the IT Rules) which was enacted under section “43A of the IT Act”<sup>105</sup>.

The definition of “Personal Data” has been enhanced in the Bill. The definition says that “personal data” would be any data which directly or indirectly identifies a natural person. The Bill also directs any Data Fiduciary to store a copy of data (personal) on Data Centre located in India.

### **3.41.1.1 DIFFERENCES BETWEEN INDIA DATA PROTECTION BILL AND EU’S GENERAL DATA PROTECTION REGULATION**

The GDPR in terms of data regulation is not just stringent but also a comprehensive law, so much so that it has become a common noun as a data protection regulation. The Indian drafters

---

<sup>101</sup>Justice AP Shah, Former Chief Justice and Delhi High Court, ‘Report of the Group of Experts on Privacy’.

<sup>102</sup>Srikrishna Experts Committee, ‘A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians’ (2018) 2018 176 <[https://meity.gov.in/writereaddata/files/Data\\_Protection\\_Committee\\_Report-comp.pdf](https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf)>. Accessed on 23 September 2019.

<sup>103</sup>Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India And Ors.’(2017) 10 SCC 1.

<sup>104</sup>MA Yadugiri and Geetha Bhasker, ‘The Information Technology Act, 2000’ (2011) English for Law 482.

<sup>105</sup>“The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011(2011) 3”.



appointed under Justice B N Srikrishna<sup>106</sup> for the purpose of preparing a draft legislation has repeatedly referred to GDPR in the draft of the Bill as well as the White Paper released by the committee. The Indian Bill is on the same lines as GDPR in terms of lawful processing, consent etc. There are few differences as well.

- (1) Indian Bill does not require to share names and categories of personal data recipients by the “Data Fiduciary” with the “Data Principle”.
- (2) In the Indian Bill “Data Fiduciary” has no obligation to share how long the data will be kept and stored with the “Data Principle”.
- (3) “Data Fiduciary” has no obligation to share the origin/source of data with the “Data Principle”.
- (4) Under Indian Bill there is no obligation to share presence of automated decision making by the “Data Fiduciary”. Under European GDPR “Data Subject” has to be provided with a copy of the data that is undergoing any sort of processing.
- (5) “Data Subject” under GDPR is required to be served with a copy of “data that is being processed”. Whereas on the other hand Indian Bill just asks for the summary of such data.
- (6) When there has been a case of data breach, Indian Bill, does not require to share such information with “Data Principle”. The decision regarding this would be taken by “Data Protection Authority”.

### **3.41.1 Brazil**

#### **General Data Protection Law ("LGPD")**

Brazil approved the LGPD on August 14, 2018<sup>107</sup>. The LGPD provided for an 18-month transition period and came into effect in 2020. Under this law data protection regime was established which defined rules for storing as well as processing “personal data” both physical and electronic.

---

<sup>106</sup>Experts Committee (n 102).

<sup>107</sup>de Souza and others (n 86).

Under the Brazil (LGPD) law, consent has to be obtained from the “Data Subject” before processing any “personal data”, this provision is similar to the European GDPR. Under the said law consent has to be obtained in such a manner, whether in writing or any other means that it clearly indicates the will of the “Data Subject”. The subject over his data must have easily accessible information which should be made available in “clear, adequate and ostensible manner.

#### Key Provisions in Comparison with the GDPR.

<b>Provision</b>	<b>LGPD</b>	<b>GDPR</b>
<b>Definition of Sensitive Personal Data</b>	Under this law Sensitive Personal Data is defines on similar lines as that of GDPR. Sensitive Personal Data includes data related to religious beliefs, health, sexual orientation which deeply identifies natural person. <sup>108</sup>	Under GDPR Sensitive Personal Data has been defined under Article 9 to include special category data revealing sensitive personal information of a man’s life. It can be related to biometric, religious beliefs, sexual orientation etc. <sup>109</sup>
<b>Whose Information is Protected?</b>	Natural persons resident in Brazil. <sup>110</sup>	Natural persons resident in the European Union.
<b>Case where Consent can be waived</b>	When “Data Subject” have already made their personal data public.	No similar exemption.
<b>Processing Children’s Data</b>	While processing the data of children a separate and specific consent has to be	The GDPR clearly defines that for a child below 16 years consent from parent is

<sup>108</sup> Artur Potiguara Carvalho and others, ‘Big Data, Anonymisation and Governance to Personal Data Protection’, *ACM International Conference Proceeding Series* (2020).

<sup>109</sup> Microsoft (n 1).

<sup>110</sup> de Souza and others (n 86).

	obtained by the parent or guardians. The law does not define the age wherein parental consent is required. <sup>111</sup>	an obligatory requirement.
<b>Anonymized Data</b>	Under Article 12, it is stated that any data even if it is anonymized will be considered as “personal data” when it can be used to build behavior profiles of an individual. <sup>112</sup>	GDPR has no provision related to anonymized data. GDPR defines "pseudonymization", under this the data cannot be attributed to a specific person without adding any information to the existing data. The additional information if available is kept separately and the organization has to make sure that personal data is not merged with such additional information still pseudonymize personal data does not change the definition or status of personal data, and, thus, remains same and within the ambit of GDPR. <sup>113</sup>

<sup>111</sup>de Souza and others (n 86).

<sup>112</sup>ibid.

<sup>113</sup>Microsoft (n 1).

### 3.41.3 Japan

In Japan the rights of individual in relation to their personal data came into effect in the year 2005. But as per the increase in the use of technology and focus of organizations shifting towards more and more use of “big data” which was the root cause for the transfers of data cross border. All this change led to the requirement of amendment in law, therefore Protection of Personal Information<sup>114</sup> (“APPI”) was amended and came into force on May 30, 2017. “Personal Information” under APPI has been defined which shall include religion, race, personal information, medical history etc. This personal information has potential to bring about prejudice. The law applies to organization and businesses who are using information of people in Japan to offer goods and services, no matter if information of citizens is dealt with in Japan or outside, APPI shall apply. This act makes consent a necessary requirement for using Sensitive Personal Information. Taking consent is not enough under this law “explicit purpose” should be mentioned by Data Handlers.

### 3.41.4 Singapore

Personal Data in Singapore is protected under Personal Data Protection Act, 2012<sup>115</sup> (“PUPA”). The act came into effect in different phases. First on 2<sup>nd</sup> January, 2013 Personal Data Protection Commission was formed. After that Do Not Call Registry<sup>116</sup> was implemented. Finally, on 2<sup>nd</sup> July, 2014 Data Protection Rules were implemented.

Under this law “Personal Data” is defined as “Data” about an individual whether true or false and the individual can be easily identified with the help of such data, the access of such data is held by the organization. The Data Protection law in Singapore has extraterritorial reach. Even though consent under Singapore

---

<sup>114</sup>Hideo Yasunaga, ‘Protection of Personal Information in Real-World Data in Japan’ (2020) *Annals of Clinical Epidemiology* 177.

<sup>115</sup>Benjamin Wong Yongquan, ‘Data Privacy Law in Singapore: The Personal Data Protection Act 2012’ [2017] *International Data Privacy Law*.

<sup>116</sup>“Warren B Chik, ‘The Singapore Personal Data Protection Act and an Assessment of Future Trends in Data Privacy Reform’, *Computer Law and Security Review* (2013).”

law is an explicit requirement, still there are quite a few exceptions as well. For example, data been used for “artistic or literary purpose”, data already available in public etc.

There is a provision under Singapore law which is totally in contrast with GDPR<sup>117</sup>, the way how consent is dealt under PDPA, Section 15 is unique. This Section provides that if a person voluntarily gives data without giving actual consent to an organization, it is considered valid procedure under law. On the other hand, under GDPR it is mandatory that consent must be unambiguous, explicit, expressed and free. Thereafter an Amendment Bill was also passed in November 2020.

### **3.41.5 Hong Kong**

Personal Data Privacy ("Ordinance")<sup>118</sup> governs data protection in Hong Kong. There are “6 Data Protection Principles” mentioned in the ordinance which governs the privacy and data of individual. Under the said law “Personal Data” is defined as data through which a person can be identified and also such data can be accessed in practicable form. The personal data under the Hong Kong law starts from name, address, medical records, identity card, employment record etc.

There are major differences when we compare EU GDPR with Hong Kong law. GDPR has wide applicability whereas the Ordinance of Hong Kong applies to personal data that is “collected, processed and used” in or from Hong Kong.

Consent provisions are also very different in Hong Kong. Consent under the Ordinance is not a “pre-requisite” for obtaining personal data. The Ordinance also doesn’t have any provision related to parental consent nor does there is any

---

<sup>117</sup>“Graham Greenleaf, ‘Asia-Pacific Free Trade Deals Clash with GDPR and Convention 108’ [2019] SSRN Electronic Journal.”

<sup>118</sup>Rebecca Ong, ‘Data Protection in Malaysia and Hong Kong: One Step Forward, Two Steps Back?’ (2012) Computer Law and Security Review 403.

requirement of breach notification to be given. The law under GDPR imposes heavy fine and penalty whereas under the Ordinance Section 50 Privacy Commission cannot impose fines or penalties first an Enforcement Notice to data handlers if they do not comply penalties are prescribed. There has been a discussion paper which proposes amendments to this Ordinance.

### 3.41.6 Canada

Canada has exhaustive law to protect right to privacy, also to see effective working and compliance of these laws there are several organization and agencies. In Canada there are two acts in relation to privacy, these acts are enforced by Privacy Commissioner-:

- (a) “Privacy Act”- Information handled by federal government.
- (b) Personal Information Protection and Electronic Documents Act<sup>119</sup> ("PIPEDA")- How businesses, organizations will use and handle personal information.

Key areas where the PIPEDA and the GDPR differ:

<b>Provision</b>	<b>PIPEDA</b>	<b>GDPR</b>
<b>Consent</b>	Consent is essential under PIPEDA. Under Section 6(1), the agreement of an individual to whom the organization's activities are directed is required on additional grounds, such as the individual's knowledge of the nature, purpose, and consequences of the	In contrast to the situation in Canada, where permission is the exclusive basis for collection, use, and disclosure (with limited exceptions), the GDPR allows for the acquisition of personal data on other bases, such as the fulfilment of a contract or legitimate interests. The GDPR lacks a notion of

<sup>119</sup>Derek Lackey and Neil Beaton, ‘The Current State of Data Protection and Privacy Compliance in Canada and the USA’ (2019) Applied Marketing Analytics 84.

	collection, use, or disclosure of their personal information. PIPEDA has no stated consent requirement. However, Consent is in accordance with Sensitivity of the data and how the individual expects how his/her information will be handled, Schedule 1, cl. 4.3.5). <sup>120</sup>	implied consent as well.
<b>Consent of Children</b>	Privacy Commissioner suggested that Children below age of 13 will not be able to give consent which is meaningful consent in such cases consent must be taken from parents and guardians. <sup>121</sup>	The GDPR has set the minimum age of consent at 16 years of age.
<b>Data Breach Reporting</b>	As of November 1, 2018, organisations subject to (PIPEDA) are required to report to the Privacy Commissioner of Canada breaches of security safeguards involving	All breaches are to be notified within 72 years.

<sup>120</sup>Lisa M Austin, 'Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA' (2006) University of Toronto Law Journal 203.

<sup>121</sup>The Office of Privacy Commissioner of Canada, 'Summary of Privacy Laws in Canada' (*Summary of privacy laws in Canada*, 2018).

	<p>personal information that pose a real risk of serious harm to individuals, notify affected individuals about these breaches, and maintain records of all breaches. There is no prescribed time and the notification to individuals is to be sent as soon as</p>	
<p><b>Data Protection Authority</b></p>	<p>Under PIPEDA, the federal Privacy Commissioner may make non-binding recommendations to organizations but cannot issue binding orders or levy administrative fines.</p>	<p>The supervisory authority possesses investigative powers (e.g., to conduct data protection audits), corrective powers (e.g., to issue warnings and reprimands, to order an organisation to bring processing operations into compliance with the GRPR, and to order an organisation to notify affected data subjects of a data breach), and advisory powers (e.g., to accredit certification bodies, to adopt standard data protection clauses, and to approve binding corporate rules).</p>
<p><b>Fines</b></p>	<p>The Federal Court may impose fines of up to \$100,000 if: I an employer fires, suspends, demotes,</p>	<p>Depending on the circumstances, administrative fines of up to: €20 million;</p>



	<p>punishes, harasses, or otherwise discriminates against a whistleblower employee; or (ii) an employer retaliates against a whistleblower employee. (iii) where a person obstructs the federal Privacy Commissioner during an inquiry or audit.</p>	<p>4% of annual worldwide turnover (whichever is higher)</p>
--	--	--

**3.41.7 United States**

**US Health Insurance Portability and Accountability Act (HIPAA)**

Both the GDPR and HIPAA<sup>122</sup> share several commonalities. These are extremely comprehensive sets of regulations and are committed to the goal of protecting privacy. Both regulate how protected information/data is collected, used, disclosed, maintained, transmitted, disposed of, kept secure, etc. Under both the regimes, individuals/data subjects can exercise comprehensive rights about their data/information.

	<b>GDPR</b>	<b>HIPAA</b>
<b>Consent</b>	Permits the use of health-related personal data with the subject's express permission, unless EU or	PHI use or disclosure can only be made after receiving an authorization from the individual such authorization

<sup>122</sup>Wilnellys Moore and Sarah Frye, ‘Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules’ (2019) Journal of Nuclear Medicine Technology 103.

	<p>member state legislation prohibits the use of consent. Under “Explicit consent” the consent taken for processing must be of higher value and standard when compared to the consent obtained for processing other forms of A person must be explicitly informed of how their data will be used and must take deliberate action to indicate their permission.</p>	<p>includes number of elements.<sup>123</sup></p>
<p><b>Employment, social security, and social protection responsibilities</b></p>	<p>Allows the Sensitive Personal Information to be processed when there arises an obligation under any collective agreement in relation to employment, social security etc<sup>124</sup>.</p>	<p>The law allows to the extend permissible by law. Usually processing of such data is prohibited for employment purposes<sup>125</sup>.</p>
<p><b>Protecting vital interests when the subject is</b></p>	<p>Protecting the interests of Data Subjects who are physically or legally incapable of providing</p>	<p>Permission has to be obtained from the representative of an individual who is incapable of giving of giving consent by</p>

<sup>123</sup>Ozgur Kafali and others, ‘How Good Is a Security Policy against Real Breaches? A HIPAA Case Study’, *Proceedings - 2017 IEEE/ACM 39th International Conference on Software Engineering, ICSE 2017* (2017).

<sup>124</sup>Electronic Frontier Foundation, ‘Genetic Information Privacy’ (2020) GINA, HIPAA and Genetic Information Privacy 55.

<sup>125</sup>Michele E Gilman, ‘Five Privacy Principles (from the GDPR) the United States Should Adopt To Advance Economic Justice.’ (2020) *Arizona State Law Journal* 74.

<b>incapable of providing consent</b>	permission may necessitate the processing of sensitive personal information. <sup>126</sup>	himself/herself.
<b>Not-for-profit entities</b>	Entities that are not-for-profit are entitled to process data even if they use it for political, intellectual, religious, or trade union purposes. The processing of member or former member data must be controlled, and such data may not be transmitted to a third party without prior authorization.	No such provision.
<b>Information already made “public” by the subject</b>	Data that has been made accessible to the public by the Data Subject may be handled by the entities.	Differs from the GDPR in that such use or disclosure by the Data Subject has no bearing on the HIPAA safeguards. <sup>127</sup>

**3.41.8 California**

California (CA), on June 28, 2018, passed a data privacy law that grants consumers greater control over their personal information. This law was subsequently amended in September 2018. The AB 375 or the California Consumer Privacy Act of 2018 ("California Act" or the "CCPA") which goes

<sup>126</sup>S Alder, A Kelleher and S Greene, ‘HIPAA Compliance Guide’ (2017) HIPAA Journal 118.

<sup>127</sup>Merrick and Ryan (n 53).

into effect on 1 January 2020, is being hailed by many as one of the strictest online privacy laws in the United States. Upon the implementation of the California Act, businesses will be required to comply with extra restrictions regarding the processing of the personal information of California residents. Before a business can collect any personal information, the California Act requires the business to inform the consumer of the categories of information it will collect and the purpose for which it will be used (including any sale). Businesses are also required to provide an online privacy policy that provides: (1) a description of the consumers' right to know, right to equal service and price; (2) methods for submitting requests pursuant to their right to know; and (3) a list of the categories of personal information it has collected, sold or disclosed in the past 12 months or the fact that it has not sold or disclosed any personal information. Businesses that sell personal information must have a prominent link on their site labelled Do Not Sell My Personal Information and enable customers to opt out of having their information sold to third parties. Few important points to note here:

- (i) The law comes into effect from January 1, 2020.
- (ii) It offers citizens of California the right to ban the sharing of personal information, the right to seek access and deletion, and the right to statutory damages for security breaches without demonstrating injury.
- (iii) The Act allows the Attorney General of California to adopt regulations after collecting public opinion.
- (iv) It mandates the delivery of personal information gathered, sold, exchanged, or otherwise revealed during the previous twelve (12) months.
- (v) It is expected to be changed by legislation submitted during the 2019-2020 legislative session.

### *Applicability*

The California Act applies to all 'businesses' that serve California residents and has a wide definition of the term "Business" which means<sup>128</sup>:

- (i) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organised or operated for the profit or financial benefit of its shareholders or other owners, that collects the personal information of consumers, or on whose behalf such information is collected, and that alone, or jointly with others, determines the purposes and means of processing consumers' personal information, and that conducts business in the United States.
- (ii) Has annual gross revenues in excess of \$25,000,000; Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices; Receives 50 percent or more of its annual revenues from the sale of consumers' personal information.
- (iii) The word "Business" also encompasses an entity that manages or is controlled by a business (as described above) and that has similar branding with the business (defined as a shared name, service mark, or trademark).

Some important points to note about the applicability of the CCPA are<sup>129</sup>:

- (a) The law does not require that one should have physical operations in California.
- (b) It applies to any entity that controls or is controlled by a "business" as defined above.
- (c) It applies to parent companies and subsidiaries sharing "common branding".

---

<sup>128</sup>Lothar Determann, 'New California Law Against Data Sharing' [2018] Computer Law Review International.

<sup>129</sup>Nicholas F Palmieri, 'Who Should Regulate Data? An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws' (2020) Hastings Science and Technology Law Journal 554.

(d) It exempts I non-profit organisations that do not operate for profit or financial gain; (ii) healthcare providers governed by California's Confidentiality of Medical Information Act (CMIA) or covered entities governed by the Health Insurance Portability and Accountability Act (HIPAA); (iii) consumer reporting agencies to the extent that their use of personal information is limited by the federal Fair Credit Reporting Act (FCRA).

## **Comparison with the GDPR**

In certain ways, the CCPA and the GDPR are comparable, but they're not the same. Both terms have wide meanings when it comes to personal data/information. Both of these pieces of law add formal compliance requirements to the protection of personal data and information. Both may result in significant regulatory fines and penalties.

There are, however, a lot of distinctions. Here's a rundown of the distinctions<sup>130</sup>:

- (i) Unlike the GDPR, California's data protection regulations are neither repealed or replaced by the CCPA.
- (ii) The CCPA provides safeguards depending on where a person lives.
- (iii) Processing of personal information is not prohibited by default under the CCPA.
- (iv) Data minimization is not required under the CCPA.
- (v) Businesses are not obligated to maintain records under the CCPA.
- (vi) Appointment of a Data Privacy/Protection Officer or an equivalent is not required under the CCPA.
- (vii) No right to correction exists under the CCPA.
- (viii) International transfers are not subject to any particular limitations under the CCPA.

The table below sets, out a comparison between the key provisions of the California Act with the GDPR;

---

<sup>130</sup>Sahara Williams, 'CCPA Tipping the Scales: Balancing Individual Privacy with Corporate Innovation for a Comprehensive Federal Data Protection Law' [2021] Indiana Law Review 114.

Provision	California Act	GDPR
<b>Definition of Personal Information</b>	The word "personal information" is defined more broadly under the California Act. Personal information is defined as data that identifies, relates to, characterizes, is capable of being connected with, or might reasonably be linked, directly or indirectly, with a specific consumer or household.	"Any information pertaining to an identified or identifiable natural person" is included in the GDPR's wide definition. The California Act, on the other hand, includes categories like as education information and business information that are not covered by the GDPR.
<b>Where is Information protected?</b>	The CCPA protects "consumers," who are defined as natural people "resident" in the state of California.  Note: While the CCPA claims to include workers who live in California, AB 25 would change the definition of "consumer" to exclude employees, contractors, agents, and job seekers.	Natural persons resident in the EU.
<b>Opting out vs Opting In</b>	Consumers must "opt out of having their data sold", and businesses must offer a user-friendly method for	For processing to take place, the data subject's explicit permission is needed.

	submitting opt-out requests.	
<b>Requirement for Data Processing</b>	Unlike the GDPR, the California Act states that data cannot be processed when a consumer has opted out, but it does not specify particular circumstances in which data may be handled.	When there is a particular legal basis, such as consent, contract fulfillment, protecting a person's vital interests, public interest, or the controller's or a third party's legitimate interest.
<b>Right of Data Subjects</b>	<ul style="list-style-type: none"> <li>• Right to be informed of the types of information collected and the purposes for collection.</li> <li>• Right to access<sup>131</sup> the categories, sources, and specific pieces of information collected, the purposes for data collection, and third parties with whom the data has been shared.</li> <li>• Right to request deletion of personal information<sup>132</sup>.</li> <li>• Right to opt out of the sale of a consumer's</li> </ul>	<ul style="list-style-type: none"> <li>• Right to be informed of data processing practices.</li> <li>• Right to access personal data and other information about processing.</li> <li>• Right to rectification.</li> <li>• Right to be forgotten.</li> <li>• Right to restrict processing.</li> <li>• Right to data portability.</li> <li>• Right to object to processing.</li> <li>• Right not to be subject to a decision based solely on automated processing.</li> </ul>

<sup>131</sup>ibid.

<sup>132</sup>ibid.



	<p>personal information<sup>133</sup>.</p> <ul style="list-style-type: none"> <li>• Right to receive services<sup>134</sup> on equal terms.</li> </ul> <p>Contrary to what the GDPR sets forth, “the CCPA does not mandate data minimization, nor does it impose the right to rectify / correct personal information”.</p>	
<b>Processing of Information of a Child</b>	<p>A business cannot knowingly sell data of a customer under the age of 16 unless<sup>135</sup>:</p> <ul style="list-style-type: none"> <li>• the consumer is between the ages of 13 and 16; or</li> <li>• the parent or guardian of the child is under the age of 13 has opted in to the sale.</li> </ul>	<p>It is legal to process children's data if the kid is at least 16 years old; else, parental permission is needed. The GDPR also allows member states to reduce the age of parental permission to no less than 13 years old.</p>
<b>Fine</b>	<p>Between \$100 to 750 per consumer each occurrence for private causes of action, or actual damages, whichever is higher.</p> <p>Civil fines of up to \$7,500</p>	<p>Administrative penalty of up to €20 million or 4% of the preceding year's worldwide annual revenue, depending on the violation.</p>

<sup>133</sup>ibid.

<sup>134</sup>ibid.

<sup>135</sup>Kimberly Dempsey Booher and Martin Robins, ‘American Privacy Law at the Dawn of a New Decade (and the CCPA and COVID-19): Overview and Practitioner Critique’ (2020) SSRN Electronic Journal 44.

	<p>per violation for CAG acts.</p> <p>Specifications:</p> <p>Businesses may suffer civil fines of up to \$7,500 per purposeful violation and \$2,500 per accidental violation in actions conducted by the California Attorney General; corporations would have thirty (30) days to fix any alleged violation after receiving notice of the alleged violation.</p> <p>In private proceedings, consumers may seek statutory damages of not less than \$100 and not more than \$750 per consumer per occurrence, or actual damages (regardless of whether actual losses have been shown), whichever is larger.</p> <p>In private proceedings, consumers may seek declaratory or injunctive relief, as well as any other</p>	
--	--	--

	<p>remedy the court deems appropriate.</p> <p>In any case initiated by the California Attorney General, companies might be subject to an injunction.</p>	
<b>Transfer of Data Between Countries</b>	The California Act does not contain any relevant restrictions in this regard.	Adequacy measures are necessary for any nation found to have legislation that differ from those of the EEA.
Data Processors	If the business wishes to exclude the transfer of personal information to the business from the definition of the sale of personal information, it must enter into a written agreement with the third party. If the service provider exemption is satisfied, the company may continue to share information with them even if the California resident expresses a desire for their personal information not to be sold.	Controllers must enter into a written contract with processors that handle a data subject's personal data that meets specific conditions.
Data Breach Notification	The California Act, unlike the GDPR, does not	A privacy breach must be reported to the data subject

	require a company to notify a customer of a data breach.	within 72 hours by the Controller <sup>136</sup> .
<b>Higher Charges for Opt Out</b>	Consumers who opt out of having their data sold can pay a greater fee as a result of the California Act.	No equivalent provision in the GDPR.
<b>Incentives for Data Sale</b>	Businesses have the right to provide non-monetary incentives in return for reselling a customer's personal data.	No equivalent provision in the GDPR.

Personal information is defined more broadly under the CCPA than it is under California's breach reporting legislation (described below). It's worth noting that the CCPA's definition of personal information is broader than the GDPR's in that it includes "household" (despite the fact that the CCPA doesn't define "households"). Personal information as defined by the CCPA excludes the following information<sup>137</sup>:

- (i) Publicly available information (data from federal, state, or municipal government records that is lawfully made available).
- (ii) customer data that has been "de-identified" or aggregated.
- (iii) information gathered, utilized, sold, or disclosed under the GLBA or the Driver's Privacy Protection Act (1995), but only to the extent that the CCPA "conflicts" with those statutes.

<sup>136</sup>Elif KiesowCortez, 'Data Breaches and GDPR', *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (2020).

<sup>137</sup>Jeeyun (Sophia) Baik, 'Data Privacy against Innovation or against Discrimination?: The Case of the California Consumer Privacy Act (CCPA)' (2020) *Telematics and Informatics* 67.

- (iv) When personal information is "reported in, or used to generate," a consumer credit report, it is sold to or from a consumer reporting agency (as defined in the Fair Credit Reporting Act or the FCRA).

Here's a quick rundown of the most important CCPA regulations for businesses:

- Inform the public about the collection practices.
- Make a statement of customers' rights available and keep it up to date at least once every twelve (12) months.
- Separately list all categories of personal information that was collected, sold, or revealed for a business purpose in the last twelve (12) months.
- Give advance notice of all onward transfers.
- Make two or more designated means for submitting requests for information available to consumers to help them with their requests.
- Implement and maintain adequate security measures, methods, and practices to ward off the private right of action created by California Civil Code Section 1798.150.
- If you're selling personal information, give people the option to opt out via a prominent link that says, Don't Sell My Personal Information.
- If selling, get consent from customers aged 13 to 16, as well as parents if the consumer is under 13.

To achieve CCPA compliance, businesses must establish privacy teams and key points of contact, as well as secure an adequate funding for CCPA compliance initiatives.

- Conduct assessments to establish the components of a CCPA compliance program that is appropriate.
- To comply with the CCPA's standards, create and update privacy policies, practices, and notices.
- Raise awareness of the CCPA and provide CCPA training.

- Create and update privacy notices and consent protocols, taking into account the unique requirements for kids' personal information.
- Create and improve ways to address the privacy rights of consumers.
- Make data breach and incident response protocols and keep them up to date.
- A data mapping exercise should be carried out.
- Create and update procedures for third-party management and sourcing.
- Ensure that suitable and acceptable security controls are implemented and maintained.
- Set up proper monitoring and testing procedures to ensure CCPA compliance.

As part of a deal with the sponsor of a similar privacy ballot measure that had qualified to be brought before state voters on Election Day in November 2018, the California Act was approved in an extremely expedited timetable. The sponsor had agreed to withdraw his ballot initiative if the California Act was signed into law before the June 28 withdrawal deadline. Given the speed at which the legislation was passed, it is certain that amendments to the legislation will be necessary in the next year and a half and it will be interesting to see the final shape that the legislation takes.

#### **3.41.8.1 Incident & Breach Management — California Data Breach Notification Law**

An entire part should be dedicated to the data privacy/security event and breach management system. First, let's look at California's Data Breach Notification Law.

- (iv) If you do business in California.
- (v) Own or licence electronic data.
- (vi) The data contains personal information of California residents (hereafter referred to as CA Residents); There was unauthorised access to electronic personal information of CA Residents; and, The personal information is not encrypted; you are required to provide a data breach notification under this law

Personal information is defined by California law as an individual's first name or first initial and last name combined with any one or more of the following:

- your social security number;
- the number on your driver's license or identification card;
- account or card numbers, whether they're used in conjunction with a security or access code;
- health-related information
- information on health insurance; or
- Information gathered through a computerized license plate recognition system.

A username or email address, as well as a password or security question and answer, are examples of personal information that would allow access to an online account. Who needs to be informed? Any CA resident whose personal information has been compromised as a result of a data breach must be notified. Any company that is compelled to notify more than 500 California residents as a result of a single data breach must additionally send a single copy of the breach notice to the Attorney General of the state. If there has been actual or suspected unauthorized access to personal information, businesses that maintain (but do not own or license) the information must notify the entity that owns or licenses the information of any security breach.

The following information should be included in the aforementioned notification:

- the person sending the notice's name and contact details;
- a list of the different forms of personal data exposed in a data breach;
- the important dates related to the breach (a timeline);
- whether the delay in giving the notice/notification is due to a law enforcement agency's inquiry;
- abroad or high-level description of the breach;
- contact information for “major credit reporting agencies” (CRAs) in the event that a social security number, driver's license number, or CA ID card number was revealed in the hack; and
- an offer to provide relevant security measures, such as identity theft prevention and mitigation services, if the organization notifying you is also the source of the incident.

A corporation can also give information about what has already been done to safeguard victims of the breach, as well as any advice on how victims can protect themselves, at its discretion.

It's how all of the above information is presented those matters. The following rules must be adhered to:

- It must be written in basic and straightforward language.
- The title must be Notice of Data Breach.

It should be divided into the following sections:

- What went wrong?
- What information was compromised as a result of the breach?
- What exactly are you up to? What can the victim do?
- More information is available.



- All titles and headings must be shown "clearly and conspicuously."
- The font size must not be less than ten points.

The importance of the notification's timing cannot be overstated. Any corporation that possesses or leases computerised data containing personal information about California residents must tell impacted individuals as soon as is practicable and without undue delay. A business or organisation that stores digital data that belongs to or is licenced by another business or organisation must tell the owner of the breach "immediately upon discovery."

All notifications must take into account the justified need to collaborate or cooperate with law enforcement, as well as the procedures necessary to analyse the scope of the breach and restore the reasonable integrity of the data system. If a law enforcement agency believes that providing such notice may compromise an ongoing criminal investigation, the notice may be postponed. It should be noted that if a notification is to be delivered to more than 500 California residents, a copy of the notification must also be shared with the California Attorney General; however, no timetable is given.

The notification(s) must be sent in writing or electronically, as long as they comply with the provisions of the federal E-Sign Act, 15 U.S.C. 7001 et seq. If the cost of delivering notification exceeds \$250,000, the number of people to be notified exceeds 500,000, or the business/company lacks appropriate contact information, notification can also be issued via a substitute notice.

The following information must be included in this substitution notice:

- An email notice (if the business/company possesses email addresses for the data subjects who are impacted);
- A prominent posting of the notice on the company's website (assuming the company has one) for at least thirty (30) days; and
- All major state-wide media are notified.

### 3.42 The Privacy Shield

The US Department of Commerce, the European Commission, and the Swiss Administration, respectively, designed the EU-US and Swiss-US Privacy Shield Frameworks<sup>138</sup> to in support of transatlantic commerce, offer a system for enterprises on both sides of the Atlantic to comply with data protection regulations when moving personal data from the European Union and Switzerland to the United States. The European Commission declared the EU-US Privacy Shield Framework acceptable to allow data transfers under EU law on July 12, 2016<sup>139</sup>. The Swiss Government declared on January 12, 2017 that the Swiss-US Privacy Shield Framework had been approved as a competent legal method for complying with Swiss standards for transferring personal data from Switzerland to the US.

#### (i) *Self-Certification I*

The Privacy Shield programme, which is administered by the International Trade Administration (ITA) of the U.S. Department of Commerce, allows U.S.-based companies to join one or both of the Privacy Shield Frameworks in order to benefit from the adequacy findings.<sup>140</sup> To join any "Privacy Shield Framework," a U.S.-based organisation must self-certify to the Department of Commerce and publicly pledge to comply with the Framework's rules.<sup>141</sup> Joining a privacy shield is a voluntary commitment, but once made, it is enforceable under US law.

During the self-certification process, an organization must submit information such as a description of its personal data privacy policy, the statutory body with jurisdiction to investigate claims against the organization for possible unfair or deceptive practices and violations of privacy laws or regulations, annual revenue, and contact information.

---

<sup>138</sup>Xavier Tracol, 'EU-U.S. Privacy Shield: The Saga Continues' (2016) Computer Law and Security Review.

<sup>139</sup>Privacy Shield Framework, 'Privacy Shield | Privacy Shield', *Privacy Shield Framework (USA, Europe)* (2018).

<sup>140</sup>Doron S Goldstein and others, 'Understanding the EU-US "Privacy Shield" Data Transfer Framework' (2016) *Journal of Internet law* 198.

<sup>141</sup>*ibid.*

(ii) *The Privacy Shield*

Framework through the EU US Privacy Shield Framework and the Swiss UID Privacy Shield Framework, the US Department of Commerce, according to its legislative power, established the Privacy Shield Principles and Supplemental Principles (collectively, "Principles"). Among these are<sup>142</sup>:

Notice: Before an organisation uses or processes such information for a purpose other than that for which it was originally collected or processed by the transferring organisation, or discloses it for the fiduciary purpose, a notice must be provided in clear and conspicuous language.

The notification must include<sup>143</sup>:

- information about the organization's involvement in the Privacy Shield; the organization's participation in the Privacy Shield.
- the organization's participation in the Privacy Shield; the organization's participation in the Privacy Shield; and the organization
- a list of the several forms of personal information gathered.
- a description of the reason for the data collection.
- a person's right to access his or her personal information.
- Whether it is<sup>144</sup>: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States, the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual.
- submitting to the FTC's, the Department of Transportation's, or any other authorized statutory authority in the United States' investigative and enforcement powers.

---

<sup>142</sup>Martin A Weiss and Kristin Archick, 'U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield', *The European Union: Challenges and Prospects* (2016).

<sup>143</sup>Article 29 Data Protection Working Party, 'Opinion 01/2016 on the EU-U.S. Privacy Shield Draft Adequacy Decision'.

<sup>144</sup>Sam Curry, 'Achieving GDPR Compliance Post-Privacy Shield' (2021) *Computer Fraud and Security* 403.

- a person's right to invoke binding arbitration under specific circumstances.
- an obligation to disclose personal data in response to authorized requests from public authorities, such as to meet national security or law enforcement requirements; and
- its responsibilities in the event of third-party transfers.

Choice: The Principles require an organization to give individuals the option of opting out of having their personal information disclosed to a third party or<sup>145</sup> used for a purpose that is materially different from the purpose(s) for which it was collected or subsequently authorized by the individuals. Individuals must be given clear, visible, and easy-to-access tools to exercise their freedom of choice.

For sensitive information, organisations must get explicit express agreement (opt in) from people (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information specifying the sex life of the individual).

Accountability for Onward Transfer<sup>146</sup>: The Principles require organisations to enter into a contract with the third-party controller stating that the data may only be processed for limited and specified purposes consistent with the individual's consent, that the recipient will provide the same level of protection as the principles, and that the recipient will notify the organisation if it makes a mistake.

Security<sup>147</sup>: Taking into account the risks inherent in the processing and the nature of the personal data”, the organization is obligated to take reasonable and

---

<sup>145</sup>U.S. DEPARTMENT OF COMMERCE, ‘Privacy Shield’, *Privacy Shield Framework (USA, Europe)* (2016).

<sup>146</sup>Dewi Sinta Hermiyanty, Wandira Ayu Bertin, ‘Guide to the EU-U.S. Privacy Shield’ (2019) *Journal of Chemical Information and Modeling*.

<sup>147</sup>Laura Drechsler, ‘What Is Equivalent? A Probe into GDPR Adequacy Based on Eu Fundamental Rights’ (2019) *Jusletter IT*.

suitable measures to safeguard it against “loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

**Data Integrity and Purpose Limitation:** Personal data must be limited to the purpose for which it was obtained, and the organization must take reasonable means to ensure that personal data is accurate, full, and current for its intended use.

Individuals must have access to their information and be able to edit, update, or delete it if it is inaccurate or has been processed in a way that violates the principles (with limited exceptions).

**Recourse, Enforcement, and Liability:** Organizations must have independent recourse processes in place to respond to individual complaints and requests for information from the Department about the Privacy Shield.

**On Uncertain Footing: The Privacy Shield?** On June 26, 2018, the European Parliament voted on a motion that questioned the efficacy of the EU-US Privacy Shield. According to the resolution, the current Privacy Shield arrangement does not provide the adequate level of protection required by Union data protection law and the EU Charter, as interpreted by the European Court of Justice, and unless the United States is fully compliant by 1 September 2018, the European Parliament requests that the Commission suspend the Privacy Shield until the US authorities comply. In response to the resolution, Vera Jourova, the EU Commissioner for Justice, wrote a letter to US Commerce Secretary Wilbur Ross on July 26, 2018, stating that the US has three months to comply with EU demands regarding the sharing of private data pertaining to EU citizens, and demanding that the US appoint an ombudsman to deal with privacy-related complaints from EU citizens. As of yet, there has been no announcement on the Privacy Shield's suspension. To add to the commotion, a coalition of technology and industry organizations sent a letter to US Secretary of State Rex Tillerson on August 20, 2018, urging him to appoint a Privacy Shield ombudsperson. The

fate of the Privacy Shield will be intriguing to watch, as will whether the EP decision leads to changes in US domestic data privacy laws.

The GDPR has more stringent regulations than the Privacy Shield. On Friday, anything you do remotely in Europe will be subject to GDPR in its entirety, and Privacy Shield will no longer be considered a "free pass" for US companies to use the data as they want, according to Giovanni Buttarelli, the EU's Data Protection Chief, to the EU Observer. Organizations in other Non-EU nations that deal with data of EU residents must comply with the GDPR, and Non-EU countries must overhaul their existing legislation to ensure that their data protection laws are deemed "sufficient" by the European Commission.

### **3.43 Conclusion**

The GDPR is now the most stringent data protection regime in the world with most other countries regarding it as the "gold standard". As seen in the table above, the number of data protection laws is expanding globally, with many being modelled after the EU Directive, the GDPR, or the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. According to UNCTAD's data protection tracker, 107 nations (of which 66 were emerging or transition economies) have enacted data protection and privacy laws. Less than forty percent of nations in Asia and Africa have enacted legislation in this area. The data may be summed up as follows:

58 percent of nations having legal provisions

10 percent of nations have legislative draughts

21 percent of nations without any laws

12 percent of nations without data

I. African continent (54 countries)

23 Legislation (43 percent)

Draft Legislation: 7 (13 percent)

Absence of Legislation: 12 (22 percent)

No Data: 12 (22 percent)

(2) America (35 countries)

Constitution: 18 (51 percent )

Draft Legislation: 8 (23%)

No Legislation: 9 (26%)

No Data (0%)

III. Asia-Pacific (60 countries)

Legislation: 27 (45%)

Draft Legislation: 4 (7%)

No Legislation: 19 (32%)

No Data: 10 (17%)

IV. Europe (45 countries)

Legislation: 44 (98%)

Draft Legislation: 0 (0%)

No Legislation: 0 (0%)

No Data: 1 (2%)

V. Least Developed Countries (47 countries)

Legislation: 17 (36%)

Draft Legislation: 3 (6%)

No Legislation: 17 (36%)

No Data: 10 (21%)

#### VI. Small Island Developing States (29 countries)

Legislation: 9 (31%)

Draft Legislation: 4 (14%)

No Legislation: 10 (34%)

No Data: 6 (21%)

Capacity of policy makers, available resources for monitoring, existing/current enforcement systems, and the existing political climate around national security—all of these have made the GDPR and OECD inspired frameworks difficult around the world. Specifically, when it comes to trade negotiations, there is increasing pressure to tone down stringency, as stringent data protection is perceived to be a barrier to trade. Additionally, there are concerns that "copy-pasting" data protection clauses from other countries will most likely not work as there are different enforcement parameters, or market surveillance infrastructure, and there are different cultural norms that are at play in different jurisdictions. We can only wait and watch for further developments in this space.



## **CHAPTER 4**

### **DATA PROTECTION REGIME IN INDIA**

*“Putting data protection at the center of digital businesses strategies is the key to improving trust and digital growth” - Steve Woods*

#### **4.1 INTRODUCTION**

Due to the mechanical inefficiency of the provisions of Information Technology Act, 2000<sup>1</sup>, the government authorities were compelled to ponder the rising concerns of privacy of individual data, which is now considered a matter of national security. The Indian government's endeavor to regulate the collection and use of personal data dates back to 2012 when the committee led by Justice A.P. Shah released its report on privacy. To fully comprehend the privacy concerns and to come up with a viable Bill to address all these issues, the Government of India formulated a data protection committee under Justice B.N. Srikrishna. The committee filed its report, commonly known as the Srikrishna Committee Report<sup>2</sup> on July 28, 2018. Thereafter, the draft Personal Data Protection Bill, 2018<sup>3</sup> was tabled in the parliament. Afterwards, a revised Personal Data Protection Bill, 2019 hereinafter referred to as PDP Bill, 2019 was introduced by the Ministry of Electronics and Information Technology in the seventeenth Lok Sabha on December 11, 2019. The committee was constituted by the Ministry of Electronics & Information Technology, Government of India. The Bill in August 2022 was withdrawn as there were many amendments suggested in the bill. Under the vision of our Hon'ble Prime Minister Shri Narendra Modi, India is moving speedily on the road of digitization, and therefore an efficient data protection law has become an essential. The Bill was broadly based on the framework of the General Data Protection Regulation (hereinafter referred to as GDPR)<sup>4</sup> of the European Union and on the principles of the landmark judgment, of the Hon'ble Supreme Court of India in Justice

---

<sup>1</sup>MA Yadugiri and Geetha Bhasker, 'The Information Technology Act, 2000' (2011) English for Law 482.

<sup>2</sup>Fair Digital Economy, Protecting Privacy and Empowering Indians, 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians Committee of Experts under the Chairmanship of Justice B . N . Srikrishna'.

<sup>3</sup>Lothar Determann and Chetan Gupta, 'Indian Personal Data Protection Act, 2018: Draft Bill and Its History, Compared to EU GDPR and California Privacy Law' (2018) SSRN Electronic Journal 576.

<sup>4</sup>Information Commissioner's Office, 'Overview of the General Data Protection Regulation (GDPR)' (2017) Information Commissioner's Office 23.

K.S. Puttaswamy (Md.) & Anr. vs. Union of India & Ors.<sup>5</sup> Bill if made effective would come in supersession of section 43A of the Information Technology Act, 2000 (the “IT Act”) and the Information Technology (Reasonable Security Practices and Personal Data or Information) Rules, 2017 (“IT Rules”)<sup>6</sup> which was enacted under section 43A of the IT Act<sup>7</sup>.

After making some amendments to the 2018 Bill, the Union Cabinet save the nod for the pending the 2019 Bill which had been referred by the parliament to a joint select committee' for review.

The Bill had widened the definition of personal data which included any data through which a natural person could be identified directly or indirectly. Furthermore, the Bill enumerated that every data fiduciaries<sup>8</sup> (any person, including the state, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data) will be required to store one serving copy of the personal data on a server or data center that is located within the territory of India.

According to the Bill, the directors or the officer- in-charge of the company shall be held liable for conduct of business of the company at the time of commission of any offence under the Bill. The data fiduciaries will also be under an obligation to conduct periodic reviews of the personal data stored-with the so that these are not retained, beyond the time period necessary for the processing of the data.

The Bill established an independent body called the Data Protection Authority of India<sup>9</sup> which shall possess all characteristics of a body corporate and shall consist of a chairperson and six whole time members.

## **4.2 PURPOSE OF THE PERSONAL DATA PROTECTION BILL, 2019**

Through this Bill, the regulation of the processing of personal data of individuals by government and private companies incorporated in India and abroad was sought. It had allowed, processing,

---

<sup>5</sup>Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India And Ors.’ (2019) 1 SCC 1.

<sup>6</sup> The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011’ (2011) 3.

<sup>7</sup>ibid.

<sup>8</sup>Julia M Puauschunder, ‘Data Fiduciary in Order to Alleviate Principal–Agent Problems in the Artificial Big Data Age’, *Information for Efficient Decision Making* (2020).

<sup>9</sup> Michael Hintze, ‘Data Controllers, Data Processors, and the Growing Use of Connected Products in the Enterprise: Managing Risks, Understanding Benefits, and Complying with the GDPR’ (2018) SSRN Electronic Journal 788.

only in case of consent or medical emergency. Exceptions to this were processing in interest of national or for lawful purpose like legal proceedings. It mandated a copy of Personal data be stored within the territory of India and critical personal data within Indian limits only. Section 14(2)(h) of the Personal Data Protection Bill, 2019 also included the operation of search engines as a possible reasonable purpose to process personal data without obtaining consent from the data subject. What is the difference between Personal data and Sensitive Personal Data?

#### **4.2.1 Personal Data**

This data pertains to a natural person who is identifiable directly or indirectly by any characteristic, trait, attribute, or any aspect of identity or combination of traits.

Section 3(28) of the 2019 Bill expanded the definition of personal data<sup>10</sup> to include a reference to online or offline characteristics, traits, attributes or any other feature of the identity of a natural person, as well as any inference drawn from such data for the purpose of profiling.

#### **4.2.2 Sensitive Personal Data**

This data related to personal data revealing, or relating to or constituting the following:

(i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status, (x) caste or tribe; (xi) religious or political belief or affiliation and (xii) any other data categorized as sensitive personal data under Section 15 of the proposed bill .

### **4.3 COMPLIANCE**

(1) Consent was mandatory for obtaining personal data, sensitive personal data, and children's data. Further, Section 34 of the Bill introduced a mandatory requirement to obtain consent from the data principal for cross-border transfer of sensitive personal data<sup>11</sup>.

(2) Clear notice was to be provided at time of collection of personal data specifying details like purpose of processing and cafe oil of personal data being collected and with whom the data would be shared.

---

<sup>10</sup> Puttaswamy (n 5).

<sup>11</sup>ibid.

- (3) Storage of personal data for the time being reasonably was necessary to satisfy the purpose.
- (4) Sensitive/ critical personal data<sup>12</sup> was to be stored in India only.
- (5) For any processing activity of personal data inside or outside India, one “mirror copy” shall be required to be retained in India.
- (6) Data fiduciary shall take steps to maintain transparency regarding general practices relating to processing of personal data. Follow principles of record keeping, data audits, data protection impact assessment.
- (7) Appoint a data protection officer as per their processing activities .
- (8) Products, systems, and processes must consider privacy-by-design concepts during development.

#### **4.4 Data Fiduciary and Data Principal**

Data Fiduciary refers to any person, whether the state, a business, a legal organisation, or an individual, who alone or in collaboration with others determines the purpose and methods of processing personal data - Article 3(13)<sup>13</sup>.

Data Principal refers to a natural person to whom the personal data referred in sub clause 28 of section 3 of the Personal Data Protection Bill, 2019 related to Section 3(14)<sup>14</sup>.

#### **4.5 Social media intermediaries (SMI)**

The 2019 Bill established standards for social media intermediaries (SMIs), i.e., an intermediary that facilitates online contact between two or more users and enables them to produce, publish, share, disseminate, alter, or access material using its services. In particular, the 2019 Bill noted that SMIs who have users above a certain threshold and whose actions have, or are likely to have a significant impact on electoral democracy, security of the state, public order, or the sovereignty

---

<sup>12</sup> Puttaswamy (n 5).

<sup>13</sup> Julia M Puaschunder, ‘Data Fiduciary in Order to Alleviate Principal-Agent Problems in the Artificial Big Data Age’ (2019) SSRN Electronic Journal 643.

<sup>14</sup> Graham Greenleaf, ‘India’s Personal Data Protection Bill, 2019 Needs Closer Adherence to Global Standards (Submission to Joint Committee, Parliament of India)’ (2020) SSRN Electronic Journal 443.

and integrity of India would be classified as significant data fiduciaries, and would be subject to the obligations relating to data protection impact assessments, record keeping, data protection officer appointment, and annual audits under sections 27-30 of the 2019 Bill. Moreover, section 93(1)(d) of the 2019 Bill outlined that the Central Government may make rules for the methods of voluntary identification to identify users of social media.

#### **4.6 Role of data fiduciary**

Under the PDP Bill 2019 personal data<sup>15</sup> could have been processed in cases where there is an expressed consent i.e. data principal has consented to such sharing; for the state to perform any function such as provision of any service or benefit to the data principal or issuance of any certifications; compliance with the law or any order/judgment of any court or tribunal; in case of medical emergencies involving health risk or threat to the life of data principal and to ensure safety of individuals during any disaster or breakdown of public order.

Data fiduciaries need to keep check on the following points while processing personal data<sup>16</sup>:

- (1) Verification of age and consent of parents is required for processing personal and sensitive personal information of children.
- (2) All breaches of data need to be reported by data fiduciaries to the authority and based on the gravity of the incident the same has to be notified to the data principal.
- (3) There must be presence of robust security controls—de-identification, encryption, prevention of unauthorized access, misuse, disclosure or destruction.
- (4) Mirror copy of personal data must be stored in India if company is 13aTed out of India.
- (5) Personal data should not be stored beyond the period necessary to fulfil the purpose of processing.

#### **4.7 Requirements**

- Notification of breach to supervisory authority
- Data Protection Officers

---

<sup>15</sup>Puttaswamy (n 5).

<sup>16</sup>Puaschunder (n 17).

- Privacy by design
- Data Protection Impact Assessment
- Records of processing activities
- Data Principal Rights

## **Requirements from Data Fiduciaries**

The following were the requirements from data fiduciaries as per the PDP Bill, 2019:

### **4.7.1 Notification of breach to the supervisory authority**

The PDP Bill, 2019 mandated the data fiduciaries and/or the data processors to immediately notify breach of any users' data, to the Data Protection Authority (DPA) where such cause harm is likely or is probable to cause harm to the 'data principal'. After that, the DPA shall determine if the user(s), whose data has been breached have to be notified or not<sup>17</sup>.

### **4.7.2 Data protection officers**

Section 301 of the PDP Bill 2019 mandated significant data fiduciaries to appoint data protection officers' who shall be the point of the fiduciary with the users i.e. the data principals and also with the DPA. The data protection officers shall advise the data fiduciary on the measures it must take to ensure compliance with the Bill and oversee that the fiduciary is not violating clauses of the Bill. The officer is also to advise the company to carry out data protection impact assessment and be responsible for the development of internal mechanisms to satisfy data principals.

### **4.7.3 Privacy by design**

The previous bill prescribed a privacy by design method, under which data fiduciaries will have to design their technical systems so as to anticipate, detect and avoid any harm to the data principal. The technology will also have to be certified and must be commercially accepted. After a data fiduciary has applied privacy by design, it may apply to the DPA for certification to get included in the innovation sandbox.

### **4.7.4 Data protection impact assessments**

---

<sup>17</sup> Charles Raab and Ivan Szekely, 'Data Protection Authorities and Information Technology' (2017) Computer Law and Security Review 77.

Section 27 provided for the significant data fiduciaries to undertake a data protection impact assessment' before processing any sensitive personal data like genetic or biometric data that may pose harm to a data principal, if disclosed without authorization. The assessment report is to contain, inter cilia, details of the planned processing, the potential harm that it possesses and methods to manage or mitigate the harm if any.

#### **4.7.5 Records of processing activities**

Section 28 of the PDP Bill, 2019 required data fiduciaries to maintain accurate and up-to-date, records of collection, transfers, erasures of personal data; keep periodic review of security safeguards; data protection impact assessments or any other aspect of processing. The 2019 Bill also enabled the users of social media who register their service from India to voluntarily verify their accounts. Such users shall be provided with a visible mark of verification.

#### **4.8 Data principle rights**

The PDP Bill, 2019 gave exclusive rights to the data principal such as:

**Right to access data Section 171:** The Bill gave the data principals the right to ask the data fiduciaries for a copy of their data stored with the fiduciaries within a specified time limit.

**Right to data correction/erasure Section 181:** The data principal was given the right to request the data fiduciary to correct any piece of data that is no longer correct. Additionally, the principal could also request the data fiduciary to erase any and all data that it might have of the user.

**Right to data portability Section 191:** The data principal was given the right to port his/her data under which he/she could ask any data fiduciary to port whatever data they have on one of the users to send to another data fiduciary.

#### **Penalties prescribed in the Personal Data Protection Bill, 2019<sup>18</sup>**

2 - 4% of total worldwide turnover, for breach of provisions in the PDP Bill or 5-15 Crore (whichever is greater)

---

<sup>18</sup> Graham Greenleaf, 'Data Protection: A Necessary Part of India Fundamental Inalienable Right of Privacy Submission on the White Paper of the Committee of Experts on a Data Protection Framework for India' (2018) SSRN Electronic Journal 661.

## 4.9 BRIEF STUDY OF THE PERSONAL DATA PROTECTION BILL, 2019

### 4.9.1 Chapter II & III - Obligations of data fiduciary and grounds for processing of personal data without consent

Section(s)	Requirements of the section
Section 11 Consent necessary before processing of personal data	<ul style="list-style-type: none"><li>• Consent of data principal is a must before the commencement of data processing.</li><li>• Consent must be<ul style="list-style-type: none"><li>- <b>Free</b>- Section 14 of Indian Contract Act, 1872</li><li>- <b>informed</b> about required information</li><li>- <b>Specific</b> in respect of purpose of processing</li><li>- <b>Clear</b></li><li>- Capable of being <b>withdrawn</b></li></ul></li><li>• The data fiduciary must not condition the fulfilment of any contract on the permission to the processing of any personal data that is not required for that purpose.</li><li>• Burden of Proof on data fiduciary - to prove valid Consent.</li><li>• The data principal is responsible for any legal ramifications resulting from a revocation of permission.</li></ul>



Section 12 -Processing of personal data without consent in certain cases<sup>19</sup>

• Personal data may be processed if deemed necessary for the following purposes<sup>20</sup>:

- The provision of any service or benefit to the data subject by the State, or the issue of any certification, licence, or authorization for any activity of the data subject by the State, is prohibited.

- Compliance with any court or tribunal decision or judgement in India.

- Medical emergency involving a threat to the life of or severe threat to the health of the data principal.

- To take steps to ensure the safety of all individuals in the event of a calamity or breakdown of public order.

• Operation of search engineer is also included in the list of ‘reasonable purposes’ Section 14(2)(h)

Section 13 –

Processing of

Personal data necessary for purposes related to employment etc.

• Personal data may be processed if it is necessary for:

- Recruitment or termination of employment of data principal by the data fiduciary.

• Any function of the state authorized by law for:

- Benefit to the data principal; or

- Any certification, license or permit for any action or activity of the data principal.

Section 14 –

• Personal data may be processed without taking

---

<sup>19</sup>Sandeep Mittal I.P.S., ‘The Role of Consent in Legitimising the Processing of Personal Data Under the Current EU Data Protection Framework’ (2017) SSRN Electronic Journal 78.

<sup>20</sup>ibid.

Processing of personal data for other reasonable purposes.

consent if such processing is necessary for reasonable purposes

- Reasonable purposes may include:
  - Prevention and detection of unlawful activity.
  - Mergers and acquisitions.
  - Whistle blowing.
  - Network and information security.
  - Credit scoring.
  - Debt recovery;
  - Processing publicly available personal data
  - Operation of search engines.
- Authority which specifies a reasonable purpose shall also lay down certain regulations to safeguard and protect the rights of data principals.

Section 15 –

Categorization of personal data as sensitive personal data <sup>21</sup>

After consultation with authority and sectorial regulator concerned, the Central Government may notify sensitive personal data to be that:

- Processing of which may cause significant harm to the data principal.
- Category of personal data which has an expected confidentiality factor.

---

<sup>21</sup>Lindsey Norman, ‘An Overview of the Changing Data Privacy Landscape in India’ (2018) 119 919 <[www.pwc.in](http://www.pwc.in)>. Accessed on 7 September 2019.

- Processing of which can cause harm to a class of data principals.

Table 4.1: Obligations of data fiduciary and grounds for processing of personal data without consent<sup>22</sup>

#### 4.9.2 Chapter IV - Personal data and sensitive personal data of children

Section(s)	Requirements of the section
Section 16 –  Processing of personal data and sensitive personal data of children <sup>23</sup>	<ul style="list-style-type: none"> <li>• Child means a person who has not completed eighteen years of age. [Section 3(8)]</li> <li>• Data fiduciary to verify age and obtain consent from parent or guardian before processing any personal data of a child.</li> <li>• Concept of guardian data fiduciary: - <ul style="list-style-type: none"> <li>- Data fiduciary who operates commercial websites or online services directed at children .</li> <li>- Process large volumes of personal data of children.</li> </ul> </li> <li>• Guardian data fiduciary shall be barred from profiling, tracking or behaviorally monitoring of, or targeted advertising directed at children and undertaking any other processing of personal data 'that can cause significant harm to the child .</li> <li>• Guardian data fiduciary providing exclusive counselling or child protection services to a child</li> </ul>

<sup>22</sup> Anirudh Burman, 'Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?' 39.

<sup>23</sup> Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' (2017) Information and Communications Technology Law.

shall not require obtaining the consent of parent or guardian of the child.

Table 4.2: Personal data and sensitive personal data of children

### 4.9.3 Chapter V - Data Principal rights (rights of individuals whose personal data are processed)

Section(s)	Requirements of the section
Section 17 - Right to confirmation and access	<ul style="list-style-type: none"><li>• Obtain confirmation that the data fiduciary is processing has processed personal data of the data principal.</li><li>• Obtain a summary of the personal data.</li><li>• Obtain a brief summary of processing activities undertaken.</li><li>• The information as required should be clear and in concise manner.</li></ul>
Section 18 - Right to correction, etc. <sup>24</sup> .	<p>The data principal shall have the right to obtain</p> <ul style="list-style-type: none"><li>• Correction of inaccurate or misleading personal data.</li><li>• Completion of incomplete personal data; and</li><li>• Updating of personal data that is out of date.</li><li>• Adequate justification in writing for rejecting the application for above changes by data fiduciary</li></ul>

---

<sup>24</sup>Shah, Justice and Court (n 2).

- Change, if not satisfied with the jurisdiction.

Data fiduciary shall also take reasonable steps to notify all relevant entities to whom personal data may have been disclosed about changes.

Section 19 - Right to data portability

- The data principal shall have the right to receive personal data in a structured, commonly used and machine-readable format.

- Above requirement is not applicable where –

- processing is necessary for functions of the state; - processing is in compliance of law.
- request would reveal a trade secret of any data fiduciary.
- it would not be technically feasible

Section 20 - Right to be forgotten

- The data principal has the right to restrict or prevent continuing disclosure where-

- data has served the purpose for which it was made.
- consent has been withdrawn; or
- is contrary to any law

- Above restriction not allowed if that was overridden by the right to freedom of speech and expression and the right to information.

Section 21 — General conditions for the exercise of rights.

- Data principal shall make a request in writing to the data fiduciary either directly or through a consent manager

- Data principal may need to pay a certain fee as specified.
- If request is refused by the data fiduciary, the reason for such refusal has to be provided to the data principal in writing.
- The data fiduciary is not obligated to comply with any request made that shall harm the rights of any other data-principals.

Table 4.3: Data Principal rights (rights of individuals whose personal data are processed)<sup>25</sup>

#### 4.9.4 Chapter VII – Transfer of personal data outside India (norms for cross-border transfer of personal data)<sup>26</sup>

Section(s)	Requirements of the section
Section 33 – Restrictions on cross-border transfer of personal data <sup>27</sup>	<ul style="list-style-type: none"> <li>• Sensitive personal data may be transferred outside India, but such sensitive personal data shall continue to be stored in India</li> <li>• Explicit consent of the data principal should be taken before transfer of sensitive personal data outside India except in the case where such transfer is made pursuant to a contract or intra-group scheme approved by the authority<sup>28</sup>,</li> <li>• Such contract/schemes should contain effective</li> </ul>

<sup>25</sup>Greenleaf, 'India's Personal Data Protection Bill, 2019 Needs Closer Adherence to Global Standards (Submission to Joint Committee, Parliament of India)' (n 18).

<sup>26</sup> Pavel Khorev and Andrey Chernetsov, 'The Problem of Ensuring Cross-Border Personal Data Transfer and Methods for Its Solving', *2020 5th International Conference on Information Technologies in Engineering Education, Inforino 2020 - Proceedings* (2020).

<sup>27</sup>ibid.

<sup>28</sup>ibid.

protection of the rights of data principal

- Every data fiduciary shall store at least one serving copy of personal data on a server or data center located in India — central government can exempt certain categories of personal data but not sensitive personal data.
- Critical personal data, as specified by central government, shall only be processed in a server or data Centre located in India.

Table 4.4: Transfer of personal data outside India (norms for cross-border transfer of personal data)

**4.9.5 Chapter VIII- Exemptions Processing of personal data in the following categories shall not be permitted unless it is authorized by a law made by parliament and state legislature and is necessary for, and proportionate to, such interests being achieved:**

Section(s)	Requirements of the section
Section 35	Security of the state
Section 36 <sup>29</sup>	<ul style="list-style-type: none"><li>• Prevention, detection, investigation, and prosecution of contraventions of law for the time being in force.</li><li>• such disclosure of personal data as is necessary for enforcing any legal right.</li><li>• such processing of personal data or by any court or tribunal in India is necessary for exercising judicial, function etc.</li></ul>

---

<sup>29</sup>Saharsh Saxena, 'Right to Privacy and The Personal Data Protection Bill of 2019: A Critique' (2021) SSRN Electronic Journal 433.

Section 37 <sup>30</sup>	Central government can exempt certain data processors by notification, for processing of personal data of data principals not within the territory of India, including any company incorporated outside the territory of India, by data processors and incorporated under Indian law
Section 38	Research, archiving or statistical purposes; however personal data shall not be processed in a manner that gives rise to a risk of significant harm to the data principal.
Section 39 <sup>31</sup>	Manual processing by small entities.
Section 40	<ul style="list-style-type: none"> <li>• Creation of sandbox for the purpose of encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest.</li> <li>• Section 40(3) states the essentials for data fiduciary applying for inclusion in sandbox.</li> </ul>

Table 4.5: Exemptions processing of personal data in the following categories shall not be permitted unless it is authorized by a law made by parliament and state legislature and is necessary for, and proportionate to, such interests being achieved

#### **4.9.6 Chapter X - Penalties and compensation (remedies for unauthorized and harmful processing)<sup>32</sup>**

Section(s)	Requirements of the section
Section 58 – Penalty for failure to comply	INR Five thousand for each day during which such default continues, subject to a maximum of ten lakh rupees in case

---

<sup>30</sup> Dr Anusuya Yadav and Gaurav Yadav, ‘Data Protection in India in Reference to Personal Data Protection Bill 2019 and IT Act 2000’ (2021) IARJSET 88.

<sup>31</sup>Saxena (n 29).

<sup>32</sup>Greenleaf, ‘Data Protection: A Necessary Part of Indiaas Fundamental Inalienable Right of Privacy Submission on the White Paper of the Committee of Experts on a Data Protection Framework for India’ (n 18).



with data principal requests under Chapter V.

of significant data fiduciaries and INR five lakh in other cases.

Significant data fiduciary - Defined under Section 26(1), the Authority can regarding the following factors notify any data fiduciary or class of data fiduciary as significant data fiduciary based on:

- volume of personal data processed.
- turnover of the data fiduciary.
- use of new technologies for processing.
- sensitivity of personal data processed.
- risk of harm by processing and
- any other factor causing harm from such processing.

#### Section 59

Penalty for failure to furnish report, returns, information, etc.<sup>33</sup>

INR ten thousand for each day during which such default continues, subject to a maximum of twenty lakh rupees in case of significant data fiduciaries and INR five lakh in other cases.

#### Section 60

Penalty for failure to comply with direction or order issued by the authority [u/s 51] or order issued by the authority [u/s 54]<sup>34</sup>

Data fiduciary or data processor shall be liable for INR twenty thousand for each day during which such default continues, subject to a maximum of INR two crores and in case of a data processor it may extend to INR five thousand for each day during which such default continues, subject to a maximum of INR fifty lakhs.

---

<sup>33</sup>Puttaswamy (n 5).

<sup>34</sup>ibid.

Section 61- Penalty for Maximum of INR one crore in case of significant data contravention where no fiduciaries, and a maximum of INR twenty-five lakh in all separate penalty has been other cases provided.<sup>35</sup>

Table 4.6: Penalties and compensation (remedies for unauthorized and harmful processing)

#### 4.9.7 Chapter XIII - Offences (protect the autonomy of individuals in relation to their personal data)

Section(s)	Requirements of the section
Section 82 – Re-identification and processing of de-identified personal data	<ul style="list-style-type: none"> <li>• Any person who, knowingly or intentionally or recklessly re-identifies personal data which has been de-identified by a data fiduciary or a data processor.</li> <li>• Without the consent of such data fiduciary or data processor.</li> <li>• Without express consent of the data principal</li> </ul> <p>Punishment – for a term not exceeding three years or fine which may extend up to rupees two lakh or both. Not liable for punishment if the personal data belongs to the person charged with the offence.</p>
Section 83 – Offences be cognizable and non-bailable.	Notwithstanding anything contained in the Code of Criminal Procedure, 1973, an offence punishable under this Act shall be cognizable and non-bailable.
Section 84- Offence by companies	Any offence committed by a company - every person who, at the time when offence was committed was in charge of, and was responsible to, the company for the

---

<sup>35</sup>ibid.

conduct of business of the company, as well as the company, shall be deemed guilty of the offence and shall be liable to be proceeded against and punished accordingly

Company means anybody corporate and includes - a firm an association of persons or a body of individuals whether incorporated or not.

Section 85 –  
Offences by state

Any offence committed by any department or authority or body of the state - the head of such department or authority or body shall be deemed to be guilty and liable to be proceeded against and punished accordingly.

Notwithstanding anything contained in this section, the provisions of Code of Criminal Procedure, 1973 relating to public servants shall continue to apply.

Table 4.7: Offences (protect the autonomy of individuals in relation to their personal data)

#### **4.10 Data Protection Authority of India**

The Personal Data Protection Bill, 2019 proposed to notify an authority called the Data Protection Authority of India (hereinafter, referred to as Authority). The Authority shall be a body corporate vested with the power to acquire, hold and dispose of property, both movable and immovable. It may also enter into a Contract and can sue or be sued.<sup>36</sup>

The Authority shall consist of a chairperson and not more than six whole-time members out of which one shall be a person having qualification and experience in law. The chairperson as well as the members of the authority shall have qualification and specialized knowledge and experience of not less than ten years in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration or related

---

<sup>36</sup>Rupal Rautdesai and others, 'Big Data and Privacy - A Legal Perspective and Comparative Study of the USA and India' (2019) International Journal of Process Management and Benchmarking 203.

subjects Section 42(4)<sup>37</sup> The chairperson and members of the Authority shall be appointed for a period of five years or till they attain the age of sixty-five years whichever is earlier and are not eligible for re-appointment. Furthermore, any vacancy caused in the office shall be filled up within three months from the date such vacancy occurred.

The primary objective of this Authority was to protect the interests of the data principals, prevent misuse of personal data and to ensure the compliance with the Bill. The Authority may also conduct activities to Promote awareness about data protection. Chapter IX of the Bill discussed extensively about the Data Protection Authority of India.

#### **4.11 DIFFERENCES BETWEEN PERSONAL DATA PROTECTION BILL, 2019 AND EU'S GENERAL DATA PROTECTION REGULATION**

The European Union's General Data Protection Regulation (GDPR) has almost become a common noun for personal data protection regulation, not just for the stringent provisions that it contained but also for comprehensiveness, of the issues that it addressed. The Indian panel was created to draft data protection legislation, under Justice B N Srikrishna who referred to GDPR repeatedly in a whitepaper it was released on November'18. While most of the areas such as had a clear purpose of processing of personal data, consent, other rights, appointment of data protection officers in organizations were taken directly from GDPR provisions, but there were a few differences.<sup>38</sup>

(1) Indian draft legislation do not require the data fiduciary as in GDPR, to share the names and categories recipients of the personal data with the data principal.

(2) There was no obligation on data fiduciary to share with the data principal the period for which the data will be stored while collecting or at any time, as GDPR mandates.

---

<sup>37</sup> Sheshadri Chatterjee, 'Is Data Privacy a Fundamental Right in India?' (2019) International Journal of Law and Management 303.

<sup>38</sup>Diana Lee, Gabe Maldoff and Kurt Wimmer, 'Comparison: Indian Personal Data Protection Bill 2019 vs. GDPR' (2020) IAPP.

(3) The data fiduciary do not need to share the source of the personal data to the data principal in case the data had not-been collected from him/her which is an explicit requirement in GDPR

(4) Unlike GDPR, there is no requirement that the data fiduciary share with the data principal the existence of automated decision making, including profiling.

(5) GDPR required that the data subject (data principal) to be provided with a copy of the data undergoing processing. The Indian legislation mandated a summary of that data to be shared, with no definition of what that summary is.

(6) In case of a breach, there was no requirement by Indian draft bill to share it with the data principal; rather, the Data Protection Authority would determine whether such breach was reported to the data principal or not. This was also in contrast to GDPR provisions<sup>39</sup>

(7) The provision that attracted the most criticism—as well as the only dissent note from one of the members—was the issue of where the personal data resides. Every data fiduciary would ensure the storage, on a server or data Centre located in India, of at least one serving copy of personal data to which this Act applied, says the Bill. The draft Bill also mentioned that the central government would notify categories of personal data as critical personal data that shall only be processed in a server or data Centre located in India. GDPR leaves this to specific countries most of which have chosen to allow free flow of data<sup>40</sup>

(8) PDP divides the data into 3 major categories – personal data, sensitive personal data and critical data. The PDP bill do not define critical data and it is the discretion of central government to declare any data as critical data. However, GDPR distinguishes data between 'special categories of data' and 'personal data' only.

(9) PDP focused mainly on the protection and regulation of data rather than enabling its cross-border flow. Sensitive personal data collected, shared or disclosed to the data fiduciary in India had to be stored within the territory of India but could be processed outside India also but

---

<sup>39</sup> Poulomi Sen, 'EU GDPR and Indian Data Protection Bill: A Comparative Study' (2021) SSRN Electronic Journal 85.

<sup>40</sup> 'India's New Data Protection Bill: Based on GDPR, But Different' (2020) Computer Law Review International 223.

critical data could not be transferred across borders of India and thus had to be stored in India mandatorily. While in GDPR, the data gets similar protection once it moves out of jurisdiction of GDPR.

(10) In PDP, the distinction of types of data holds relevance regarding the storage purpose and the data can be stored within territory of India for longer duration with the permission of data principle or if required by any law or obligation. While, in GDPR, the data is required to be kept in an identifiable form for the duration required for the specified purpose and the exception to increase duration are public interest, scientific or historical relevance.

(11) PDP do not incorporate the immediate right to restrict the processing which provides a window to stop the processing, while the claim of other rights was still a challenge. However, under GDPR, a data subject has the right to limit or restrict the processing of his/her data.

(12) The PDP do not provide for any certification mechanism unlike GDPR which provides for data protection seals and marks to ensure that data controllers and data processors are compliant with regulation for purpose of international data transfer.

(13) The PDP do not provide for any compensation to the person suffering material or non-material damages from the infringement of obligations unlike GDPR which has a provision.

One of the recent cases of GDPR is of British Airways, in which it was facing fine of £183 million for 2017 breach of its security systems. The website of the airline was diverted to a fraudulent site and details of about 500,000 customers were stolen. Variety of information was “compromised” by poor security arrangements including names, email addresses, credit card information such as credit card numbers; expiry dates and the CVV code and address information<sup>41</sup>.

Information Commissioner Elizabeth Denham said:

People's personal data is just that - personal. When an organization fails to protect it from loss, damage or theft, it is more than an inconvenience. That's why the law is clear - when you are

---

<sup>41</sup> ICO, ‘Intention to Fine British Airways £183.39m under GDPR for Data Breach | ICO’ (*Information Commissioner’s Office*, 2019).

entrusted with personal data, you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights.

Fine was imposed under new law i.e., the General Data Protection Regulation (GDPR). It was the biggest shake-up to data privacy<sup>42</sup> in 20 years. It also increased the maximum penalty to 4% of turnover. In the present case the penalty amounts to 1.5% of its worldwide turnover in 2017”, less than the possible maximum.

#### **4.12 STATUTES / RULES / CONVENTIONS COVERED**

Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011<sup>43</sup>

- These rules mentioned the necessary reasonable practices a body corporate had to follow to keep the personal and sensitive data of the user secure.
- Rule 4-Body corporate had to provide Policy for Privacy and disclosure of information. Clear and easily accessible statements of its practices and policies had to be provide by the body corporate<sup>44</sup>.
- Rule 5-While collecting information consent from the provider of information was to be mandatorily taken and other similar guidelines mentioned in the rules was need to be followed while collecting information<sup>45</sup>.
- Rule 6-Prior consent of third parties was required while disclosing their information, except in case, where government agencies were mandated to do so as per law<sup>46</sup>.
- Rule 7-Mentioned certain guidelines which were needed to be followed while transferring information<sup>47</sup>.

---

<sup>42</sup> Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, ‘The European Union General Data Protection Regulation: What It Is and What It Means’ (2019) Information and Communications Technology Law 654.

<sup>43</sup>The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (n 8).

<sup>44</sup>ibid.

<sup>45</sup>ibid.

<sup>46</sup>ibid.

Information Technology [The Indian Computer Emergency Response Team and Manner of Performing Function and Duties] Rules, 2013

- The Indian Computer Emergency Response Team (CERT-In), would serve as the national agency for performing certain functions in the area of cyber security like:
- Collection, analysis and dissemination of information on cyber incidents; forecast and alerts of cyber security incidents; and emergency measures for handling cyber security incidents.
- Rule 12(1)(a)- If anybody corporate, data Centre and intermediary come across any cybersecurity issue, they would have to report to the CERT-In team as early as possible. Information Technology Act, 2000<sup>48</sup>
- Section 43A-Defines body corporate and lays penalty on such body for failure to protect data”.<sup>49</sup>

A privacy policy is an essential piece of information both for customers to know and for organizations to make known. In simpler terms, a privacy policy helps in communicating the way in which an organization handles personal data and/or sensitive personal data which they may acquire from individuals over a period of time or for some purpose. A privacy policy is technically a legal document and efforts should be made to draft the document in a way that is both easy to understand and is accurate.

The provisions of applicable laws in India including the Information Technology Act, 2000 and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011<sup>50</sup> makes it compulsory for organizations to maintain privacy of personal data that they collect.

The basic sections which would form a part of the structure of a privacy policy could be the following:

---

<sup>47</sup>ibid.

<sup>48</sup>ibid.

<sup>49</sup>Rishab Bailey and Smriti Parsheera, ‘Data Localisation in India: Questioning the Means and Ends’ (2019) SSRN Electronic Journal 112.

<sup>50</sup> The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011’ (n 8) .



- (i) An introduction: This part of your policy can tell your visitors about your organization.
- (ii) Data privacy: This part of your policy can contain information about the storing of —
  - (a) Personal data: This may include the name, contact details including residential address, date of birth, details of documents such as Aadhaar/PAN/ voter ID/ passport.<sup>51</sup>
  - (b) Sensitive personal data: This may include financial information such as bank account or credit /debit card details, biometric information, any details pertaining to financial information, sexual orientation, medical records etc. provided to the body corporate for providing any service.
  - (c) Usage of personal data: This section states the way in which an organization shall use personal data e.g., facilitating transactions, reporting transactions, sharing updates on product/service changes etc.
  - (iii) Sharing of data: This part of the policy shall explain about the parties with whom data may be shared with. This may include third parties who perform services on behalf of the organization, sharing of data in compliance with a court order, to comply with a law in force or at the request of a government agency or investigatory body.
  - (iv) Cookie policy: A “cookie” is a small piece of information stored by a web server on a web browser so it can be later read back from that browser<sup>52</sup>.
  - (v) Appointment of grievance officer<sup>53</sup>: In accordance with the Information Technology Act, 2000 and rules made there under, the name and contact details of the grievance officer shall be provided. Rule 3(11) of The IT (Intermediaries Guidelines) Rules, 2011 states about the appointment of grievance officer.

## **4.13 Categorization of Data**

### **4.13.1 Sensitive personal data or information [SPDI]**

---

<sup>51</sup>Frederike Kaltheuner and Elettra Bietti, ‘Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR’ (2018) *Journal of Information Rights, Policy and Practice* 323.

<sup>52</sup>Ignacio N Cofone, ‘The Way the Cookie Crumbles: Online Tracking Meets Behavioural Economics’ (2017) *International Journal of Law and Information Technology* 303.

<sup>53</sup>Greenleaf, ‘Data Protection: A Necessary Part of Indiaas Fundamental Inalienable Right of Privacy Submission on the White Paper of the Committee of Experts on a Data Protection Framework for India’ (n 18).

As per the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules 2011, Sensitive personal data or information [SPDI] of a person means such personal information which consists of information relating to password, financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history, biometric information; any detail relating to the above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing - stored or processed under lawful contract or otherwise.

Freely available or accessible information or information furnished under the Right to Information Act, 2005 or any other law for the time being in force has been expressly excluded from the definition.

#### **4.13.2 Personal data or information [PDI]**

The 'Rules' Further define 'Personal information' [PM] as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, can identify that person.

#### **4.13.3 Major provisions involved**

- Section 43A of “The Information Technology Act”, 2000.
- Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011.
- Information Technology [The Indian Computer Emergency Response Team and Manner of Performing Function and Duties] Rules, 2013.

#### **4.14 MANDATORY COMPLIANCE**

<b>S.No.</b>	<b>Name of Act/ Rule</b>	<b>Section/Rule</b>	<b>Key Features</b>
1	Information Technology	Rule 4 — Body corporate	Policy to be published on the website of the body corporate or any

[Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011.<sup>54</sup>

provide policy for person on its behalf and shall privacy and provide for- disclosure of information

- Clear and easily accessible statements of its practices and policies.
- Type of personal or sensitive personal data or information collected.
- Purpose of collection and usage of such information.
- Disclosure of information including sensitive personal data or information as provided in rule -6.
- Reasonable security practices and procedures as provided under Rule 8.

2. ...do...

Rule 5 — Collection of information while collecting information<sup>55</sup>

- Mandatory consent from provider of information while collecting information.
- Mandatory appointment of grievance officer to address complaints.
- Name and address of the agency that is collecting the information; and the agency that will retain the

<sup>54</sup>‘The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011’ (n 8).

<sup>55</sup>ibid.

3. ...do...	Rule 6- Disclosure of information <sup>56</sup>	<p>information</p> <ul style="list-style-type: none"> <li>• Disclosure to third parties require prior consent.</li> <li>• Third parties should not disclose it further</li> </ul> <p>Exception: Disclosure to certain Government Agencies mandated under law without prior permission.</p>
4. ,..do...	Rule 7 — Transfer of information <sup>57</sup>	<ul style="list-style-type: none"> <li>• Requires prior consent of provider of information.</li> <li>• Allowed only if it is an obligation under a contract.</li> <li>• Same level of data protection should be ensured</li> </ul>
5. ,..do...	Rule 8 - Reasonable security practices and procedures <sup>58</sup> .	<ul style="list-style-type: none"> <li>• International Standard IS/ISO/IEC 27001 on Information Technology/ Security Techniques/Information Security Management System approved as compliant.</li> <li>• Audit reasonable security practices and procedures by an auditor at least once a year or after every significant up gradation.</li> </ul>

---

<sup>56</sup>ibid.

<sup>57</sup>ibid.

<sup>58</sup>ibid.

<p>6. Information Technology[The Indian Computer Emergency Response Team and Manner of Performing Function and Duties] Rules, 2013</p>	<p>Rule 12(1)(a) - CERT-In operations</p> <ul style="list-style-type: none"> <li>• Targeted scanning/probing of critical networks/systems</li> <li>• Compromise of critical systems/information</li> <li>• Unauthorized access of IT systems/ data</li> <li>• Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites etc.</li> <li>• Malicious code attacks such as spreading of virus/worm/Trojan/Botnets/ Spyware</li> <li>• Attacks on servers such as Database, Mail and DNS and network devices such as Routers Identity Theft, spoofing and phishing attacks Denial of Service (DOS) and Distributed Denial of Service (DDoS) attacks • Attacks on Critical infrastructure, SCADA (Supervisory Control and Data Acquisition) Systems and Wireless networks</li> <li>• Attacks on Applications such as E-Governance, E-Commerce etc. controlled or operated by the body</li> </ul>
--	--

corporate.

- Body corporate is negligent in implementing and maintaining reasonable security practices and procedures.
- Causes wrongful loss or wrongful gain to any person.
- Body Corporate shall be liable to pay damages by way of compensation to the person so affected.

Table 4.8: Mandatory compliance under the IT Act and Rules made thereunder

#### 4.15 NON- MANDATORY BUT ESSENTIAL COMPLIANCE

S.No.	Checklist
1.	Obtain consent from all users in writing through letter or fax or email [or otherwise through any established electronic means] regarding purpose of usage before collection of such information. <sup>59</sup>
2.	Not collect sensitive personal data or information unless:  [a] the information is collected for a lawful purpose connected with a function or activity of your organization or any person on its behalf; and  [b] the collection of the sensitive personal data or information is considered necessary for that purpose.

---

<sup>59</sup> Eric Lachaud, 'ISO/IEC 27701 Standard: Threats and Opportunities for GDPR Certification' (2020) European Data Protection Law Review 128.

3. Not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any law for the time being in force
4. Permit the users, as and when requested by them, to review the sensitive personal information they have provided.
5. If your organization is required to collect, receive, possess, store, deal or handle personal information [including any sensitive personal information], it shall ensure that each such user has consented to
  - [a] such collection, receipt, possession, storage, dealing or handling of all such personal information, and
  - [b] such transfer and disclosure of the same.

Table 4.9: Essential compliance though not mandatory

While except for the Privacy Policy none of the other policies are mandatory, the following polices are still crucial so as to ensure compliance under the IT Act:

<b>S.No.</b>	<b>Policy</b>	<b>Why do we need it?</b>
1.	Data processing policy	Data Processing Policy in an organization shall explain what kind of personal data they compile and how they use it. This policy should be in clear and simple form to make it easy to understand, so that one can determine on a free and voluntary basis whether they wish to provide their personal data or those of the members of their organization.
2.	Data protection policy	Key pieces of information that are commonly stored by business houses be they employee records, customer details, loyalty schemes, transactions, or data

collection, needs to be protected. This is to prevent that data being misused by third parties for fraud, such as phishing scams, and identity theft.

Common data that your business might store, include:

Names

Addresses

Emails

Telephone numbers

Bank and credit card details

3. Data breach policy

This policy and plan will aim to manage personal data breaches effectively. An organization shall be committed not only to the letter of the law but also to the spirit of the law and place a high premium on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.
4. Terms of use

Sometimes referred to as Terms and Conditions, T&Cs, or Terms of Service, a Terms of Use policy outlines the rules a user agrees to abide by while using a service, and these will vary depending on the business or the purpose of the website/app. The information included on the T&C page might relate to intellectual property, how the organization expects people to behave in the online community, how online orders are dealt with, deliveries, returns and complaints.



5. Intellectual property policy IP rights are important because they can:
- set a business apart from competitors
  - be sold or licensed, providing an important revenue stream.

One may be surprised at the various aspects of a business that can be protected. An organization's name and logo, designs, inventions, works of creative or intellectual effort or trademarks that distinguish its business can all be types of IP.

6. Social media policy<sup>60</sup> With the rapid growth and application of social media, an organization needs to have a policy in place that ensures employees who use social media (either as part of their job or in a personal capacity), have guidance as to the company's expectations of their behavior and communication online. This is particularly important around social media usage regarding the organization, its people, partners, products or services, competitors or other individuals and organizations related to the organization. A social media policy can be an organization's first line of defense in mitigating risk for both the employer and the employee.

Table 4.10: Other essential policies helpful in protecting data

#### 4.16 USE OF VISUALS IN PRIVACY NOTICES

---

<sup>60</sup>Qiang Chen and others, 'Social Media Policies as Responses for Social Media Affordances: The Case of China' (2016) Government Information Quarterly 561.

Consent forms inclusive of privacy policies of body corporates are turning out to be ineffective resulting into users' data being collected and misused. Recently, the former judge of the Hon'ble Supreme Court, Justice B.N. Srikrishna<sup>61</sup> who has also been involved in the drafting of the new data-protection laws for India asked if giving out pictorial warnings with respect to obtaining consent will be of greater use in terms of the process of collection of data by the body corporates and any person on their behalf from the data providers? Just like the warnings we see on the cigarette packets.

The pending bill on the personal data protection will make body corporates more accountable for the collection and use of data thereby giving the users greater control over their data. Therefore, the way in which the collected data shall be handled by a particular body corporate should also be communicated to the users' right at the time of taking their consent. This will also help the data providers to understand the type of data being shared and its' audience or what type of data is being collected at a particular point of time.

Therefore, similar to the warning on the cigarette packets which warns smokers of the probable health risks involved, visuals at the time of providing data shall also give a clear warning as to how the data would be used and by whom. What becomes an essential point to ponder here is that the accountability of data collectors is not only limited to giving information to the users but also of ensuring that data providers understand the risks. Hence, creating effective privacy notices with visuals can lead to clearer and more comprehensible notices.

#### **4.17AADHAAR ACT**

Chapter VII of the Act provides for offences and penalties but does not talk about damages to the affected party<sup>62</sup>

- Section 37 states that intentional disclosure or dissemination of identity information, to any person not authorized under the Aadhaar Act, or in violation of any agreement entered into under the Act, will be punishable with imprisonment up to three years or a

---

<sup>61</sup>“Srikrishna Experts Committee, ‘A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians’ (2018) 2018 176 <[https://meity.gov.in/writereaddata/files/Data\\_Protection\\_Committee\\_Report-comp.pdf](https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf)>.” Accessed on 17 December 2019.

<sup>62</sup>Dr Ahmad Shaikh, ‘The AADHAAR Act: Is It Disturbs the Right to Privacy? A Critical Study’ (2020) SSRN Electronic Journal 187.

fine up to ten thousand rupees (in case of an individual), and fine up to one lakh rupees (in case of a company)<sup>63</sup>.

- Section 38 prescribes penalty with imprisonment up to three years and a fine not less than ten lakh rupees in case any of the acts listed under the provision are performed without authorization from the UIDAI<sup>64</sup>
- Section 39 prescribes penalty with imprisonment for a term which may extend to three years and fine which may extend to ten thousand rupees for tampering with data in Central Identities Data Repository.
- Section 40 holds a requesting entity liable for penalty for use of identity information in violation of section 8(3) with imprisonment up to three years and/or a fine up to ten thousand rupees (in case of an individual), and fine up to one lakh rupees (in case of a company)
- Section 41 holds a requesting entity or enrolling agency liable for penalty for violation of section 8 (3) or section 3 (2) with imprisonment up to one year and/or a fine up to ten thousand rupees (in case of an individual), and fine up to one lakh rupees (in case of a company)<sup>65</sup>
- Section 42 provides general penalty for any offence against the Act or regulations made under it, for which no specific penalty is provided, with imprisonment up to one year and/or a fine up to twenty-five thousand rupees (in case of an individual), and fine up to one lakh rupees (in case of a company)

Though the Aadhaar Act prescribes penalty in case of unauthorized access, use or any other act contravening the regulations, it fails to guarantee protection to the information and does not provide for compensation in case of violation of the provisions.

#### **4.17.1 Privacy policy**

---

<sup>63</sup>Amit Kumar Tyagi, G Rekha and N Sreenath, 'Is Your Privacy Safe with Aadhaar?: An Open Discussion', *PDGC 2018 - 2018 5th International Conference on Parallel, Distributed and Grid Computing* (2018).

<sup>64</sup>Anupam Saraph and Sanjana Krishnan, 'The Curious Case of PAN-Aadhaar Linkage' (2020) *Economic and Political Weekly*.

<sup>65</sup> Sheshadri Chatterjee, 'Is Data Privacy a Fundamental Right in India?: An Analysis and Recommendations from Policy and Legal Perspective' (2019) *International Journal of Law and Management* 165.

IT Rules: Rule 4 requires a body corporate to provide a privacy policy on their website, which is easily accessible, provides for the type and purpose of personal, sensitive personal information collected and used, and Reasonable security practices and procedures<sup>66</sup>.

Aadhaar Act: Though in practice the contracting agencies (the body corporates under the Aadhaar ecosystem) may maintain a privacy policy on their website, the Aadhaar Act does not require a privacy policy for the UIDAI or other actors.

Implications: Because contracting agencies will be covered by the IT Rules if they are 'body corporates', the requirement to maintain a privacy policy will be applicable to them.

#### **4.17.2 Consent**

IT Rules, 2011: Rule 5 requires that prior to the collection of sensitive personal data, the body corporate must obtain consent, either in writing or through fax or through an e-mail regarding the purpose of usage before collection of such information.<sup>67</sup>

Aadhaar Act: The Act is silent regarding consent being acquired in case of the enrolling agency or registrars. However, section 8 provides that any requesting entity will take consent from the individual before collecting his/her Aadhaar information for authentication purposes, though it does not specify the nature (written/through fax/e-mail).<sup>68</sup>

Implications: If the enrolling agency is a body corporate, they will also be required to take consent prior to collecting and processing biometrics. It is possible that since the Aadhaar Act envisages a scheme which is quasi-compulsory in nature, a consent provision was deliberately left out. This circumstance would give the enrolling agencies an argument against taking consent, by saying that the Aadhaar Act is a specific legislation which is also later in point of time than the IT Rules, and a deliberate omission of consent coupled with the compulsory nature of the Aadhaar scheme would mean that they are not required to take consent of the individuals before enrolment.

---

<sup>66</sup> Dr Govind Singh Rajpurohit and Dr Raj Kumar Yadav, 'A Socio-Legal Analysis of WhatsApp Privacy Policy 2021 in India: A Contemporary Study' (2021) SSRN Electronic Journal 67.

<sup>67</sup> Bayu Sujadmiko and others, 'The Urgency of Digital Right Management on Personal Data Protection' (2021) International Journal of Research in Business and Social Science (2147- 4478).

<sup>68</sup> AKRS Anusha, 'Privacy and Security Issues in Aadhaar' (2017) International Journal for Research in Applied Science and Engineering Technology 47.

### **4.17.3 Collection limitation**

IT Rules, 2011: Rule 5 (2) requires that a body corporate should only collect sensitive personal data if it is connected to a lawful purpose and is considered necessary for that purpose.

Aadhaar Act: Section 3(1) of the Act states that every resident shall be entitled to obtain an Aadhaar number by submitting his demographic information and biometric information by undergoing the process of enrolment.

### **4.17.4 Notice**

IT Rules, 2011: Rule 5(3) requires that while collecting information directly from an individual, the body corporate must provide the following information<sup>69</sup>:

- The fact that information is being collected
- The purpose for which the information is being collected
- The intended recipients of the information
- The name and address of the agency that is collecting the information
- The name and address of the agency that will retain the information

Aadhaar Act: Section 3 of the Act states that at the time of enrolment and collection of information, the enrolling agency shall notify the individual as to how their information will be used; what type of entities the information will be shared with; and that they have a right to see their information and tell them how they can see their information. However, the Act is silent regarding notice of name and address of the agency collecting and retaining the information.

Section 43 of The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 makes liable any companies and their management for offences committed under the Aadhaar Act, which means companies can be taken to court if individuals or a group of individuals find that there are clear violations of their personal or biometric data by employees or the company itself.

If a complaint is made against a company, then the person at the company who is responsible for that matter will be prosecuted along with the company itself. A lot of these prosecutions end up

---

<sup>69</sup>‘The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011’ (n 8).

becoming slow because law enforcement and prosecutors lack the necessary training to prosecute these complicated offences. Therefore, there is a need to upgrade the law enforcement agencies to investigate offences under Aadhaar Act. Section 47 of the Aadhaar Act, which is now scrapped, stated that only the Unique Identification Authority of India (UIDAI), or a person or officer authorized by it, could register and file criminal complaints against individuals or companies for offences under Aadhaar Act.

#### **4.18 SECTION WISE RECOMMENDATIONS OF INDIA'S PERSONAL DATA PROTECTION BILL, 2019**

1. The inclusion of “norms for social media intermediaries” in the Bill's introduction and subsequent provisions (Clause 26 which creates the category of social media intermediary and Clause 28 which allows users of a social media intermediary's services to voluntarily verify their accounts)<sup>70</sup> are outside the scope of data protection legislation and risk conflicting with provisions provided for in other legislation.

The Bill should be amended to eliminate this category and its related clauses.

2. The bill define danonymization as the irreversible process of changing or converting personal data to a form in which a data principal cannot be recognized, which satisfies the criteria of irreversibility established by the Authority in respect to personal data.

Anonymization must be defined in a way that protects privacy while still allowing for scientific study and innovation. This may be accomplished in a variety of ways<sup>71</sup>. For example, the word irreversible from the concept of anonymization may be deleted to allow for technological and scientific advancements. This would also explain the difficulties with anonymization and the capacity to re-identify people, as numerous experts, including the Sri Krishna Committee, have pointed out. Because there are numerous exclusions linked to anonymized data in their present

---

<sup>70</sup> Abu Bakar Munir and Siti Hajar Mohd Yasin, 'The Personal Data (Protection) Bill 2009' (2010) *Malayan Law Journal* 198.

<sup>71</sup> Jan Zibuschka and others, 'Anonymization Is Dead - Long Live Privacy', *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft für Informatik (GI)* (2019).

state, a high barrier is acceptable and may be used later if anonymization methods do really provide irreversibility in the future. Alternatively, we might apply the Brazilian data protection bill's definition of anonymization, which defines anonymized data as data linked to a data subject who cannot be identified, using reasonable and accessible technological methods at the time of the processing. Another option is to mandate anonymization via aggregation, with personal data no longer being protected under the Act once aggregated. Although aggregated data comes under the category of anonymized data, it may nevertheless create community privacy issues, necessitating the application of fair and reasonable processing requirements.

### 3. Clause 3 (8)

One out of every three Internet users in the world is a kid under the age of 18. Children between the ages of 15 and 24 are the most connected age group, according to the UNICEF Report on the State of the Children in 2017, and children are increasingly accessing the internet at a younger age. In some countries, children under 15 are as likely to use the internet as adults over 25<sup>72</sup>. The Justice Sri Krishna Committee recognized that a significant percentage of internet users in India are children under the age of 18, and that prescribing 18 as the age below which children must obtain parental consent would be impractical and may actually have a chilling effect on children's ability to freely use the Internet as a medium of communication.

In this respect, we would like to repeat our prior remarks. The Sri Krishna study supports making the consent age the same as the contract age by claiming that data sharing permission is often interwoven with contract consent. However, when discussing non-consensual data processing, the study defends it by saying that a person's relationship with the state cannot be reduced to a contract. It's also worth noting that the study and the bill are quiet on the status of non-consensual processing of children's data.

The parental permission requirements enable the data fiduciary to develop services that will be utilized by children without guaranteeing that their data is handled with care. This obligation should be represented in the definition as well as the concept of privacy by design contained in

---

<sup>72</sup>Charles Russo and Robert J Safransky, 'Children's Internet Protection Act', *Encyclopedia of Education Law* (2013).

Chapter VII section 29<sup>73</sup>. This would also strengthen the grounds for redress for children and parents, which are now confined to the presence of consent. With this requirement in place, the age of required permission might be lowered, and the data fiduciary may be charged with the additional task of educating minors in the most straightforward way possible about how their data would be used. When developing services that will be used by children, this method puts a duty on data fiduciaries and enables children to be aware of data processing while engaging with technology.

#### 4. Clause 3 (18)

This definition is limited in scope, including only a) account numbers or other personal data needed to identify an account, card, or payment instrument ; and b) personal data related to a financial institution's connection with a data principle, such as financial condition and credit history.

Financial statements, financial transactions, and usage of financial services provided by financial institutions should be included to the inclusive list in the second leg of the definition. We also propose that the definition include or refer to current financial information definitions, such as those contained in the Master Direction Non-Banking Financial Company Account Aggregator, without restriction (Reserve Bank) Directions, 2016 as it relates to personal information.

#### 5. Clause 3 (28)

Notwithstanding the fact that this term has been extended from the definition provided in the 2018 Bill to include and shall include any inference derived from such data for the purpose of profiling. Data about or related to a real person who may be identified directly or indirectly based on any feature.<sup>74</sup>

Any characteristic, attribute, or other aspect of such natural person's identity, or any combination of such features, or any combination of such features with any other information; or

---

<sup>73</sup>Greenleaf, 'India's Personal Data Protection Bill, 2019 Needs Closer Adherence to Global Standards (Submission to Joint Committee, Parliament of India)' (n 18).

<sup>74</sup>Yadav and Yadav (n 49).



any combination of such features with any other information. The term with respect to any characteristic, trait, attribute, or other element of such natural person's identification<sup>75</sup> defines the scope of data that is considered personal data. As a result, data that may be used to identify a natural person but does not relate to any characteristic, trait, attribute, or other aspect of that person's identity would be excluded from this definition. This would rule out information like social security numbers or other identifiers as long as they aren't combined with characteristics of a natural person's identity. Individuals may be tracked using IDs and pseudo-identifiers, which can disclose identifying information. As a result, the definition should include IDs and pseudo identifiers. Furthermore, the words identified and identifiable are not defined clearly. In this respect, the EU's Article 29 Working Party<sup>76</sup> has made suggestions that we believe are appropriate. When a natural person is differentiated from all other members of a group of people, he or she is said to be identified. A person who is natural is Identifiable implies that, despite the fact that the person has not yet been identified, it is feasible to do so using all reasonable measures available to a data fiduciary or any other person to identify the individual.

The term personal data should be broadened to encompass identifiers used to monitor natural people. An identification number kept by a data fiduciary together with other non-identifying information would not be covered by the present definition. While this definition would cover identity numbers when they are combined with any characteristic, trait, attribute, or any other feature of such natural person's identity, because identity numbers are also other information, it is important that persistent identifiers be treated differently than other types of information.

It would also be helpful to emphasize that the term encompasses any element of a person's identity. The Bill's definition of personal data matches the Article 29 Working Party's interpretation of identified and identifiable<sup>77</sup>.

---

<sup>75</sup> Rajat Misra and Rajat Grover, Future of Privacy: Evaluating the Personal Data Protection Bill, 2019 in Light of Contract for the Web (2020) SSRN Electronic Journal 77.

<sup>76</sup>Dvara Research, 'Comments to the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill 2019 Introduced in the Lok Sabha on 11 December 2019' (2020) SSRN Electronic Journal 109.

<sup>77</sup>Himanshu Arora, 'Grounds for Lawful Processing of Personal Data in GDPR and Personal Data Protection Bill 2018, India (PDPB): Section – VII: Employment Purposes' (2021) SSRN Electronic Journal 303.

Personal data is data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute, or other feature of any aspect of such natural person's identity, any identifiers intended to be associated with such natural person, any combination of such features,<sup>78</sup> we propose as an alternative definition.

The following are examples of a combination of such characteristics or identifiers with any Terms that the Bill does not specify or leaves to the Central Government or the Authority to define further:

- (a.) Data Reliability Score
- (b.) Sensitive Personal Information
- (c.) Employer-Employee Relationship
- (d.) Non-personal information

These should be specified in detail.

#### 6. Clause 5- *Limitation on purpose of processing of personal data.*

The Bill replaced the language that any person processing personal data has a duty to data principals to process their data in a fair and reasonable manner with the following: Every person processing personal data of a data principal shall process such personal data—(a) in a fair and reasonable manner and ensure the data principal's privacy.<sup>79</sup>

The use of the word duty, and had suggested that, in order to clarify the meaning of this provision and to align it with the Report's intent of protecting against harm, we believe that adding the word fiduciary will make it clear that it means processing in the interest of the data principal. Any person processing personal data has a fiduciary responsibility to the data principal to handle such personal data in a fair and reasonable way that respects the data principal's privacy and does not damage the data principal's interests.

---

<sup>78</sup>Graham Greenleaf, 'GDPR-Lite and Requiring Strengthening – Submission on the Draft *Personal Data Protection Bill* to the Ministry of Electronics and Information Technology (India)' (2018) SSRN Electronic Journal.

<sup>79</sup>Himanshu Arora, 'Grounds for Lawful Processing of Personal Data in GDPR and Personal Data Protection Bill 2018, India (PDPB): Section – I: Consent.' (2020) SSRN Electronic Journal 87.

7. Clause 5 (a) The provision in the 2018 Bill has not been modified. The Bill stipulates that the Authority has a duty to publish and give advice on the criteria of clear, specific, and lawful, when clearer definitions emerge through the Authority's evaluation of use cases. Consider the following scenario: A purpose is precise if it is explicit enough to identify what types of processing are and are not included within it. Reasons like enhancing users' experience, marketing purposes, IT-security purposes, and future research will seldom satisfy the requirements of being specific without additional information. A purpose is obvious if it is stated in such a manner that the fiduciary (including all necessary employees) and any third-party processors, as well as the data protection authority and the data principals involved, all understand it in the same way.

This section's incidental purpose requirement should be replaced with the compatible purpose standard, which states that the processing is consistent with the original reasons for which the personal data was acquired. To avoid function creep, data must be processed in a manner that is comparable to the reason for which it was acquired.

The following factors should be considered when determining compatibility: (a) the relationship between the purposes for which the data were collected and the purposes of further processing. (b) the context in which the data were collected and the reasonable expectations of the data principals regarding their further use. (c) the nature of the data and the impact of the further processing on the data; and (d) the nature of the data and the impact of the further processing on the data.<sup>80</sup>

8. Clause 6 *Limitation on collection of personal data.*

The provision in the 2018 Bill has not been altered<sup>81</sup>. This sentence should additionally include a proportionality test, such that it reads as follows: Personal data should be collected only to the extent that it is required and appropriate for the purposes of processing.

---

<sup>80</sup> Arora, Grounds for Lawful Processing of Personal Data in GDPR and Personal Data Protection Bill 2018, India (PDPB): Section – I: Consent. (n 127).

9. Clause 7(1) *Requirement of notice for collection or processing of personal data.* Specifies a provision that is quite like the provisions of the 2018 Bill<sup>82</sup>. The exceptions to the need of giving notice, on the other hand, have been extended. In two situations identified as requiring prompt action under clauses 15 and 21, namely medical emergencies, provision of services during a threat to public health, and provision of services during a disaster or breakdown of public order, data fiduciaries were not required to provide notice under the 2018 Bill.

Only the sections listed in the 2018 Bill should be exempt from giving notice. The data principal has the right to be notified in order to give informed consent, thus notification is provided. The notification should be clear and should notify the data principal of both her rights and the data fiduciary's responsibilities

According to Clause 12 (4) of this Bill, if the data principal withdraws the permission for the processing of any personal data required for the execution of a contract to which the data principal is a party, the data principal is responsible for all legal implications of such withdrawal. As a result, the notification should also inform the data principal about the nature of their connection and whether or not there is a statutory or contractual obligation. In addition, the notification should explain the implications of the failure to submit such data, as well as the right to withdraw from processing. This is comparable to GDPR Article 13(2) (e).

The data subject must also have the right to know whether the information is being used to make automated judgments about her. The lack of this privilege is justified by the fact that the DP Bill already has a mechanism for seeking legal action in the event of damage or a violation, according to the Report. However, it is critical to include this option so that this remedy may be sought directly from the data fiduciary without placing the Authority under extra strain. The data

---

<sup>81</sup>Deva M Prasad and Suchithra C Menon, 'The Personal Data Protection Bill, 2018: India's Regulatory Journey towards a Comprehensive Data Protection Law' (2020) *International Journal of Law and Information Technology* 42.

<sup>82</sup>ibid.

principal must be notified that automated decision-making, including profiling (as defined in Section 2 (33) of this Bill)<sup>83</sup>, is taking place.

**10. Clause 11. *Consent necessary for processing of personal data.***

The clause is almost identical to those included in the 2018 Bill. This paragraph specifies that permission must be obtained no later than at the start of processing; nevertheless, it may be impossible for a data principal to predict how the data will be handled in the future at the start of processing. Data may be handled by the fiduciary in ways that the data subject has not agreed to when the use of data to deliver services becomes increasingly widespread and linked to other services. Clause 30(2) says that the data fiduciary must inform the data principal through periodic notifications of significant activities in the processing of personal data. However, this clause makes no mention of obtaining permission from the data subject for the additional processing.

The blanket consent method is problematic because it takes away the data principal's authority. In 2018, the Data Protection Bill's report recommended the creation of consent dashboards to minimize consent fatigue and provide data owners more information and control over their data<sup>84</sup>. According to the study, the dashboard would offer a mechanism where the data fiduciary would be informed, and fresh permission would be sought if she had not agreed to a processing. The consent dashboard, on the other hand, will take time to establish as well as to educate the data principals on how to use it. As a result, the Bill should include minimal protections and procedures to guarantee that the data principle retains control over her data, and just providing notice will not enough.

Although the provision for withdrawal of permission may be justified as a justification, if the principle wishes to utilize the data fiduciary's service but disagrees to the new addition of processing, she only has two options: accept to the processing or withdraw from the service entirely.

---

<sup>83</sup>Himanshu Arora, 'Automated Decision Making: European (GDPR) and Indian Perspective (Indian Personal Data Protection Bill, 2018)' (2020) SSRN Electronic Journal 163.

<sup>84</sup>Rishab Bailey and others, 'Comments on the (Draft) Personal Data Protection Bill, 2018' (2018) SSRN Electronic Journal 89.

**Clause 12** may indicate that consent is necessary not only at the outset of processing, but also when personal data is being processed for a purpose that was not mentioned at the time consent was obtained. The PDP Bill's research underlines the need of preventing permission fatigue, although the data subject must be informed of and assent to each new processing operation. The data subject must be able to utilise the services for which she has provided consent while also having the opportunity to opt out of some non-service-related processing.

11. Personal data may be processed if such processing is necessary and proportionate, as an alternate wording for all of the Bill's sections dealing with non-consensual processing.

**Clauses 13 and 14** of the 2018 Bill, which dealt with non-consensual data processing, have been combined into Clauses 12 (b) and (c) of this Bill. However, it has also incorporated the reasons for non-consensual processing of sensitive personal data given by the 2018 Bill within the scope of this provision, according to Clauses 12 (c) to (f). The equivalent requirements for processing sensitive personal data in the 2018 Bill required compliance with a higher threshold. For example, processing sensitive personal data for prompt action and certain State functions had to be strictly necessary, and similarly, processing sensitive personal data in accordance with law or any order of any court could be carried out if such processing is expressly mandated by any law made by Parliament or any State Legislature or is required to comply with a court order.

The provision of all public services or benefits should not be considered a blanket exemption from the consent requirement. The Authority/Central Government may be given guidelines to identify and inform delivery of public services that enable non-consensual processing of the data principal's personal data

Nonconsensual personal data processing should be justified not only by need, but also by proportionality. The three-pronged test of need, legitimacy, and proportionality was set down in the Puttaswamy decision<sup>85</sup>. The state's non-consensual use of data for the purpose of delivering

---

<sup>85</sup>“Greenleaf, ‘India’s Personal Data Protection Bill, 2019 Needs Closer Adherence to Global Standards (Submission to Joint Committee, Parliament of India)’ (n 18).”

services to the data principal must be not only essential, but also proportionate to the execution of the state's role.

This provision now compels employers to get permission before processing sensitive personal data. However, it is unclear on what basis and by whom a determination will be made where the data principal's consent is not appropriate due to the data fiduciary's employment relationship with the data principal or would require disproportionate effort on the data fiduciary's part due to the nature of the processing. It is uncertain if the rules would apply to all kinds of labor and individuals in the workforce since it does not define the terms employment or employee, nor does it relate to a particular meaning under Indian law.

12. Clause 14 lays forth eight different reasons why personal data may be used without permission. The list had been extended with the 2018 Bill to include search engine operations. Processing must be required for this, and the choice must be evaluated against five factors. The authorities will also decide whether or not notification under section 7 is required<sup>86</sup>.

The clause mandated that the processing of personal data without permission be both essential and reasonable. Furthermore, the terms credit scoring and search engine operation be deleted from the list of possible reasonable objectives. We also suggest deleting the phrase prevention and detection of any illegal conduct, including fraud.

13. This section has been amended to allow the Central Government, in conjunction with the Authority and relevant sectoral authorities, to designate additional types of personal data as sensitive personal data based on four criteria.

The Power had exclusive authority under the 2018 Bill to further designate personal data as sensitive personal data.

---

<sup>86</sup>Saxena (n 48).

The justification for allowing the Central Government to notify categories of personal data as sensitive personal data, although in collaboration with the Authority and the sectorial regulator, is unclear. We propose that the 2018 Bill's provision be restored, and that the Authority be given the authority to decide other categories of personal data in collaboration with sectorial regulators.

14. Clause 16- When the data subject reaches the age of majority, there is no mechanism for her to withdraw her consent. The Aadhar Act was modified by the Central Government in July 2019, allowing a kid who has been enrolled in the Aadhar database by her parents/guardians to request deletion of her Aadhar within six months after turning 18.

The data principle should be able to withdraw her permission to any future processing of her data once she has reached the age of majority. According to the Act, the data principal has the right to know what personal data has been gathered on her once she has reached the age of majority. However, because this would need the gathering of data regarding the child's age, there would need to be extra safeguards in place to prevent the data from being used for further processing and profiling. Furthermore, upon reaching majority, the data fiduciary shall seek fresh consent from the data principle, and the data principal should have the opportunity to withdraw from the processing if she does not consent to future processing.

15. The data principal had the right under the 2018 Bill to get a short overview of the personal data that had been or was being processed. This has now been changed to provide the data principal access to the actual processed personal data. It also gave the data principal the ability to see the identities of the data fiduciaries with whom the data has been shared, as well as the categories of personal data shared with them, all in one location.

Also, the data fiduciary had an increased right of access, which was welcomed. It was also critical that, in addition to the right to confirmation, the data controllers be supplied with information explaining the basis for the processing. Adding sub-clause (c), which reads: an explanation of how the processing is justified under one or more of the requirements under Chapters III and IV.



16. Clause 19 (1) has been amended from the 2018 Bill, which extended this right to all data, not only data processed by automated methods. This right should be applied to all data, not only data processed via automated methods.

17. The title of this Clause should be modified from Right to be Forgotten to Right to Prevent Continuing Disclosures, and it should contain a right for individuals to request that personal information be de-indexed. The bill also establishes an adjudicating person who will receive complaints and make a judgment. To avoid privatization of regulation, the data protection Bill study supports having a central adjudicating authority the authorizing body rather than the data fiduciary. However, having a single authority to accept and adjudicate requests places a significant load on this authority, which may not be able to manage the influx of demands. Furthermore, for each request, the authority will have to coordinate with the data fiduciary, making the procedure very time intensive. This is especially important when it comes to personal data and sensitive personal data. The data fiduciary may be granted the power to delete the data in response to the data principal's complaints, and the data principal could be held responsible to an adjudicating body by giving an account and rationale for each erasure request and the cause for it.

While there should be an applaud to the Bill for giving data subjects the right to request the deletion of their personal data;

(a) There must be a right to data processing limitation.

When one of the following applies, the data principal has the right to seek from the data fiduciary a limitation of processing:

(1) The data principle contests the correctness of the personal data for a time allowing the fiduciary to verify the integrity of the personal data:

(2) the processing is illegal, and the data controller objects to the erasure of personal data and instead asks that their use be restricted; or

(3) The fiduciary no longer requires the personal data for the processing purposes, but the data subject does for the purposes of establishing, exercising, or defending legal rights.

(b) A right to object to processing must exist.

The data principal shall have the right to object to processing under Clause 13, Clause 17, and Clause 19 at any time. Upon receiving such an objection, the fiduciary must immediately cease processing the personal data unless they can show compelling reasons for processing for the purposes of establishing, exercising, or defending legal rights<sup>87</sup>.

18. Clause 22- The provision is comparable to one in the 2018 Bill; however, the Bill should emphasize privacy by default rather than privacy by design. To guarantee purpose restriction and data minimization, the Bill should include the following policy measures.<sup>88</sup>

1. The data fiduciary must take steps to ensure that only the personal information required for and proportionate to each processing purpose is gathered.

2. Data fiduciaries, particularly those that handle sensitive personal data, must adopt data minimization, and use tools like anonymization. Furthermore, while the Bill's requirement that each data fiduciary's privacy by design policy be published on their website as well as the Authority's website is commendable, this provision could be strengthened by establishing a timeframe after certification by which the policy must be published and requiring that the policy be updated and re-certified if and when significant changes occur.

19. Clause 23- From the 2018 Bill, there has been a change in language.

Information available in such form and manner as may be prescribed by regulations has been substituted for available in a readily accessible form in the current Bill.

The data fiduciary must maintain some degree of openness in order for the data principal to exercise their rights under the Bill. According to reports on company privacy policies, the length

---

<sup>87</sup> Greenleaf, 'India's Personal Data Protection Bill, 2019 Needs Closer Adherence to Global Standards (Submission to Joint Committee, Parliament of India)' (n 18).

<sup>88</sup>Spector (n 23).

and legalese render these important rules unavailable to individual consumers. As a result, we propose that the 2018 version's previous language be reinstated to ensure that the data principal is informed of their rights.

20. Clause 24- This clause requires data fiduciaries to develop security safeguards based on the associated risks and the likelihood and severity of harm, such as de-identification and encryption, data integrity safeguards, and safeguards against misuse, unauthorized access, modification, and disclosure/destruction of personal data.<sup>89</sup>

These procedures must be evaluated on a regular basis in accordance with rules. Though the inclusion of security measures in the Bill is good, considering the significance of security in the digital era, there is no clear form of accountability or baseline level for security. This may lead to a wide variety of security practices and enforcement levels developing in India, weakening overall national cyber security.

We propose that the Bill's wording mandate a yearly review rather than a periodic review, as well as an audit by an independent third party as part of the review. The findings of an audit like this should be included into a data fiduciary's data trust score. We further propose that the Bill make it mandatory to follow security standards that have been recognized and authorized at the sectorial, national, and international levels.

21. Clause 25- The provision is similar to that which was included in the 2018 Bill.

(a) The fiduciary must disclose the breach as soon as feasible as and no later than the Authority's deadline. It doesn't specify what constitutes an acceptable time span. Furthermore, the authority's duty for determining this time period is not outlined in clause Powers and Functions of the Authority. It's worth noting that the authority's powers and functions under Clause 49 do not include the authority's duty to set the time period. It has also been left out of Clause 94, which specifies the subjects for which the Authority has the authority to enact rules.

---

<sup>89</sup> Ponnurangam Kumaraguru and Niharika Sachdeva, 'Privacy in India: Attitudes and Awareness V 2.0' (2012) SSRN Electronic Journal 226.

(b) Section 32 (5) provides that, based on the seriousness of the breach, the damage anticipated to be caused to the data principal, and any mitigating action the data principal may need to take, the Authority may opt to require the fiduciary to disclose the breach to the data principal.

The Bill provides no explanation on the definitions or thresholds envisioned by these words, and it gives the Authority complete discretion over whether the data principal should be notified of a breach of his or her personal data. For two reasons, this may be problematic. First, notifying the data principal allows the person to take context-specific steps to mitigate the damages caused by the breach in his or her situation—something the Authority may not be able to discern. Second, from the standpoint of the insurance business, if breaches are not disclosed, consumers will be worried about cyber risk and therefore less likely to get insurance.

(a) Under paragraph 32(3), impose a reasonable time restriction on the data fiduciary's reporting of data breaches, or empower the Authority to set time limitations under article 60.

(b) Rather than allowing the Authority to choose when to inform the data principal of a breach, make this disclosure obligatory under paragraph 32 (5). Only carefully specified circumstances, such as national security, should be permitted for the Authority to withhold this information.

## 22. Clause- 26 (4) and 28 (3)

Clause 26 (4) empowers the Central Government in consultation with the Authority notify any social media intermediary as a significant social data fiduciary if (a) the social media intermediary has users above the threshold notified by the Central Government; and (b) the activities of the intermediary have, or are likely to have a significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India.

Clause 28 (3) further states that every social media intermediary which has been notified as a significant data fiduciary shall enable the users who register their services from India, or use their services in India, to voluntarily verify their accounts.

The classification of social media intermediaries and the verification obligation are out of the scope of a data protection legislation. Additionally, the construct of social media intermediaries as significant data fiduciaries suffers from several issues:

(a) With respect to the conditions for social media intermediaries to be designated under clause 26, the numerical thresholds are to be set with respect to the number of ‘users. The term ‘user’ has not been defined in the Bill or elsewhere in this context, and the Bill is silent on the treatment given to nonregistered users or the level of activity required to be counted as a user.”

(b) The condition requiring assessment for significant impact on electoral democracy is vague, which may incentivize social media intermediaries to implement overly-restrictive content moderation practices to avoid designation.

(c) The Authority, which has been tasked with notifying significant data fiduciaries in all other cases, has been relegated to a consultative role with respect to social media intermediaries. The rationale behind this differential treatment is not clear.

(d) Delegated law regulates voluntary user verification. Given the absence of a guiding framework in the parent Bill, the regulations announced in this respect may weaken the voluntary character of verification.

The Bill should be amended to remove provisions dealing with social media intermediaries and account verification.

23. Clause 32- The clause is almost identical to those included in the 2018 Bill. While the clause lays out the procedure for grievance resolution and the steps that must be done by the data fiduciary, it does not specify the means for filing a grievance.

A list of important mechanisms should be included in this sentence, and we propose the following alternative language: The data principal may lodge a complaint with the Data Protection Authority through online lodging, toll-free phone lines, e-mail, letter, fax, or in person.

24. Clause 33- From the 2018 Bill, this clause has been changed. There are currently no restrictions on moving personal data outside of India, instead of requiring the keeping of one serving copy of personal data inside India and a severe limitation on vital personal data and sensitive data. Sensitive personal data, on the other hand, would continue to be kept in India, and vital personal data will only be handled there.

Though the ability to transfer personal data outside of India is a welcome change, we remain concerned about the government's application of a “one size fits all” data localization requirement in a data protection bill. We would encourage the government to consider sectorial regulation around specific categories of data, such as defense-related data. We're particularly worried about the undefined category of “essential personal data,” which creates an unclear operating environment for businesses and may lead to compliance and implementation problems if the category is regularly altered.

The Bill eliminates this clause, as well as the category of essential data.

25. Clause 34- Sensitive personal data may be transmitted outside of India if certain criteria are met, such as if the transfer is made according to an authorized contract or intra-group arrangement, or if the Central Government permits it.

Critical personal data may be sent outside of India to a company that provides health services or responds to an emergency, or if the Central Government has approved the transfer. This is a shift from the 2018 Bill which allowed personal data to be sent outside of India under five circumstances and only sensitive personal data to be transferred outside India under two conditions, while critical personal data may only be handled in India.

With regard to this clause, the following is suggested:

- The intra-group schemes mentioned in this section are likely to be comparable to the GDPR's binding corporate regulations. Adequacy findings, enforceable corporate policies, express permission, standard contractual terms, and recognized codes of conduct/certification are all options available under the GDPR for international data transfers. Clause 34 seems to merge

several processes (consent, contract, and intra-group scheme) into a single mechanism, with the Central Government's permission as the sole alternative option for transfer. The government should develop a set of numerous, comprehensive procedures for transferring sensitive data outside of India.

The Authority should be the only one in charge of evaluating and approving such methods.

- Personal data should be reintroduced within the scope of this section, since the present wording excludes it, implying that it may be transmitted outside of India without guarantee that it is handled in accordance with the Bill's provisions.
- The provision should go into more detail on how each transfer mechanism would operate and what criteria must be fulfilled in order for it to be approved. For example, it is presently unclear if the provision would need the government/authority to authorize each transfer or whether the government/authority will approve an intragroup plan, after which businesses will be free to transfer data.

The data fiduciary was granted exemptions from the Bill's various provisions in cases of processing of “(i) personal data required for the State's security, (ii) prevention, investigation, prosecution, and contravention of law, (iii) processing for the purpose of legal proceedings, (iv) research, archiving, or statistical purposes, and (v) personal and domestic purposes under the 2018 Bill”. Any data fiduciary handling personal data for such defined purposes, however, was still obliged to follow the fair and reasonable processing guidelines. Similar reasons for exemptions from the different sections of the Bill have been given in the current Bill, however unlike the 2018 Bill, the exemptions from the application of the Bill's provisions have been extended to include exemption from fair and reasonable processing of personal data.

In addition, repeating our previous remarks:

- (a) The criterion of necessary and proportional for state security, or the prevention, detection, investigation, and punishment of legal violations, is too broad. While it may not be feasible to define “necessary and proportional” in detail, it would be very helpful to provide explanations that give advice on how these legal standards should be used.

- (a) There is no need or clear process for the agencies concerned to prove necessity and proportionality before a judicial or quasi-judicial body in its present form. The Authority should establish a commission to evaluate all requests for processing under Clauses 42 and 43 and be subject to their decisions.
- (b) We propose that Clauses 42 and 43 include a duration restriction, which states that data will only be kept for a certain length of time before being deleted.
- (c) The exemptions provided by Clauses 42 and 43 do not have to be as broad as they are now. Personal data breaches should be reported to the Authority, and data audits should continue to be conducted.
- (d) We further propose that users be given notification rights under Clauses 42 and 43. Such notification may be withheld if it cannot be ruled out that notifying the data subject will jeopardize the processing's purpose, or if there are any general disadvantages to the purposes under Clauses 42 and 43.
- (e) In the same way, data principals shall be given a limited right of confirmation, access, and correction when their personal data is processed under Clauses 42 and 43. These rights may be restricted if such confirmation, access, or correction jeopardizes the processing's purpose.

26. Clause 35- The exemption was granted under the 2018 Bill for the security of the state, provided that such processing of personal data was (i) allowed by law; (ii) carried out in accordance with the legislation's procedure; (iii) required; and (iv) proportional to the objectives pursued. The Supreme Court's Puttaswamy principles are enshrined in this four-stage procedure. Even though the Sri Krishna Committee's second suggestion of an ex-ante court approval of the procedure was not included in the Bill, it was seen as a first step in determining the State's surveillance capabilities.

This four-stage procedure, however, has been eliminated under the current Bill. The provision now simply states that the Central Government, if it believes it is necessary or expedient, may exempt any government agency from the application of all or any of the provisions of this Bill in respect of the processing of personal data, subject to such procedures, safeguards, and oversight mechanisms as may be prescribed, by a written order. The reasons for such an exemption have



also been broadened to encompass processes related to India's sovereignty and integrity, state security, friendly relations, and public order. These are the limitations on freedom of speech and expression imposed by Article 19(2) of the Indian Constitution<sup>90</sup>, which are currently being used to exclude personal data protection.

The Bill gave an agency of the Central Government a blanket exemption from all of the Bill's requirements; it was not limited to a specific function or purpose of the agency. Unlike the 2018 Bill, which granted exemptions from specific provisions, the current Bill grants power to exempt the agency from any or all of the Bill's provisions, thereby exempting it from the obligations set forth in Chapter XIII (offenses), Chapter X (Penalties and Compensation), and Chapter IX (General Provisions) (Data Protection Authority of India).

These rules are incompatible with an effective privacy law because they do away with the four-pronged test, which was established by the Supreme Court in . There was also no provision for either a prior judicial review of the order by a district judge, as envisaged by the Justice Srikrishna Committee Report, or a post facto review of the order by an oversight committee, as provided for by the Indian Telegraph Rules, 1951 and the Information Technology Act's rules. According to the clause, such personal data processing must follow the method, safeguards, and monitoring mechanisms that may be established. Clause 93, which gives the Central Government the authority to establish regulations on defined reasons, does not have a comparable provision.

Following in addition to the suggestions given under General comments:

- (a) The exemption should pass the four-stage criteria outlined in the 2018 Bill: (i) authorized by law; (ii) carried out in accordance with such legislation's process; (iii) need; and (iv) proportional”.
- (b) The process and safeguards should be included in the parent Bill rather than being delegated to the Central Government's regulations.

---

<sup>90</sup> Kalyani Ramnath, *We the People: Seamless Webs and Social Revolution in India's Constituent Assembly Debates* (2012) South Asia Research 118.

(c) The exemptions should not be as broad as they are now. Exemptions from Chapter XIII (Offenses), Chapter IX (Data Protection Authority of India), and security protection measures are unnecessary<sup>91</sup>.

(d) Requirements such as notifying the Authority of personal data breaches and conducting data audits shall remain in place.

e) Prior judicial review of the written order exempting the Central Government agency from the Bill's requirements.

27. Clause 36 (a) exempts personal data from certain requirements where it is handled in the purposes of preventing, detecting, investigating, and prosecuting any crime or other violation of any law in effect at the time. A condition antecedent for this provision to take effect under the 2018 Bill.

Clause 36 was

(a) a legislation passed by Parliament or a state legislature authorizing such exemptions, and (b) a law passed by Parliament or a state legislature authorizing such exemptions.<sup>92</sup>

(b) it was both necessary and appropriate to the goals that were being pursued.”

This Bill no longer has these provisions.

Furthermore, similar exemptions in regard to the processing of personal data would apply to a victim, witness, or anybody with knowledge about the crime/violation of the law under the 2018 Bill. This clause/requirement has been removed from the bill as well. The 2018 Bill further specified that after the purpose for which the personal data was processed is fulfilled, the data would be destroyed.

This clause has been removed from the current bill as well.

---

<sup>91</sup> Greenleaf, 'India's Personal Data Protection Bill, 2019 Needs Closer Adherence to Global Standards (Submission to Joint Committee, Parliament of India)' (n 18).

<sup>92</sup>ibid.

Personal data may be used under the existing law for the prevention, detection, and punishment of any crime. Because the word "offense" is not defined, even a violation of a contractual agreement may be considered an offense under this article.

Following in addition to the suggestions given under General comments:

- (a) Once the purpose for which the personal data was processed under this paragraph has been fulfilled, the personal data should be destroyed.
- (b) Reintroduction of provisions in the 2018 Bill identifying who would be affected by this clause.
- (c) Defining the word offense to encompass only cognizable offenses as established by the 1973 Code of Criminal Procedure.

28. Clause 38- In situations where personal data is handled for research, archiving, or statistical purposes, the Authority may exempt a data fiduciary from the implementation of certain requirements of the Bill under the 2018 Bill. Provisions relating to fair and reasonable processing, security measures, and data protection impact assessment have to be followed, however. The need for compliance with these clauses has been removed from the 2019 Bill.

The exclusions should be limited, and the requirements of the 2018 Bill should be restored.

29. Clause 40- The Authority will establish a sandbox to encourage innovation in artificial intelligence, machine learning, and any other new technology in the public interest.<sup>93</sup>

Any data fiduciary with an approved privacy by design policy from the Authority is eligible to apply. The sandbox will loosen standards such as purpose definition, personal data limitation, personal data retention limits, and requirements for data processing in a fair and reasonable way with permission. Data sandboxes, as stated in the General Comments, are intended to be a secure

---

<sup>93</sup> Big Data Value Association, 'Data Protection in the Era of Artificial Intelligence - Trends , Existing Solutions and Recommendations for Privacy-Preserving Technologies'.

place where only a copy of the company's or participating businesses' data is kept. It refers to a scalable and creation platform that can be utilized to investigate an organization's data collections. Regulatory sandboxes, on the other hand, are regulated settings in which companies may introduce innovations to a small client base under a loosened regulatory framework, after which they may be permitted to enter the wider market if certain criteria are met.

Sandboxes are regulatory instruments that may be used to allow businesses to develop without being burdened by excessive regulations. These usually refer to expenses associated with high entry barriers (such as capital requirements for financial and banking firms) or regulatory costs.

However, the relaxation of data protection requirements for data fiduciaries under this bill would result in individual privacy limitations . Limiting basic rights in the name of fostering innovation is not a constitutionally sound stance, and it runs counter to the main goals of data protection legislation.

30. Clause 42- The members of the Appointment Committee for the selection of members to the Authority have been substantially altered since the 2018 Bill, potentially reducing the Authority's independence significantly. According to the 2018 Bill, the Selection Committee was made up of three people (i.e, the Chief Justice of India, the Cabinet Secretary and one expert of repute). However, the current Bill has eliminated the judicial member and the expert from the Selection Committee's makeup, making it completely made up of members of the Executive.

The foundation for a solid and comprehensive data protection system in the nation is an independent Authority, therefore the Selection Committee charged with selecting the Authority must likewise be regarded as independent and impartial.

The Selection Committee's composition be reverted to the 2018 Bill's makeup. In addition, we repeat our earlier remarks: the committee will include one prominent person from the business sector and one distinguished person representing civil society.

31. Clause 43- The salary, allowances, and other terms and conditions of employment of the chairman and other members of the Authority would not be changed to their detriment throughout their tenure, according to the 2018 Bill. This clause was removed from the present bill. The Authority's members must be able to operate independently and be free of government supervision in order for it to function efficiently and smoothly. By removing the provision prohibiting the government from changing salaries and terms and conditions of appointment, the Central Government now has the power to reduce salaries or amend terms of appointment to the detriment of Authority members, effectively giving it control over the Authority's operations .

The 2018 provision should be restored, and it should be explicitly stated that the chairperson's and members' terms of appointment, wages, and allowances will not be changed to their detriment during the period of their appointment.

32. Clause 44- On the basis of the reasons stated in the Bill, the Central Government has been given the authority to remove the chairman and/or other members of the Authority from office. Given that the Authority's function as a data fiduciary requires them to exert authority over both the Central and State governments, it's important to guarantee that the power of removal does not rest exclusively with the Central Government.

A committee similar to the one established for member appointment must likewise be established to deal with any problems relating to member removal.

33. Clause 49- Unlike the 2018 Bill, the Authority's ability to define residuary categories of sensitive personal data has been eliminated in the current Bill. In collaboration with the sectoral regulators and the Authority, the Central Government has now been given this authority.

Furthermore, the Authority's powers and functions have been decreased in comparison to those stated in the 2018 Bill. The Authority's responsibilities under the 2018 Bill included in (i) issuing guidance on the Bill's provisions either on its own or in response to a query from a data

fiduciary; (ii) preparing and publishing reports detailing the results of any inspection or inquiry in the public interest; and (iii) advising the Central Government on the acceptance of any relevant international instrument relative to the Bill. The Authority's duties have been removed from the current Bill. It's unknown why these functions were removed.

The 2018 Bill's provision be restored, and that the Authority be given the authority to decide other categories of personal data in collaboration with sectorial regulators. Furthermore, the Authority's defunct powers should be restored, and it should be obliged to disclose the findings of any investigation that it considers to be in the public interest. This is helpful for (a) data principals to see how various data fiduciaries handle data protection; (b) the Authority to correct its rules and regulations as required; and (c) the Authority to gain greater confidence and openness.

34. Clause 50- The Authority had the authority to establish a code of practice addressing the method for processing personal data of users who were unable to provide valid consent under the 2018 Bill. The Authority's authority has been eliminated from the current Bill. The reason for the power's removal is unknown.

The authority to publish a code of practice in order to build an acceptable system for processing personal data of users who are unable to provide valid permission should be restored. Furthermore, we repeat our earlier remark: Academic and research organizations, especially those working on problems of privacy, security, and encryption; civil society organizations involved in research or raising awareness on privacy and data protection concerns should be included in this clause as entities that may submit codes of practice.

35. Clause 55- The Inquiry Officer may retain the confiscated material in its possession for a time not later than the completion of the investigation, according to clause 55 (4). The confiscated material may only be kept for six months under the 2018 Bill (unless the Authority approved the retention for a longer period). Furthermore, under the 2018 Bill, the individual who seized the material had the ability to create copies of it. Under the current Bill, this clause has been removed.

The confiscated materials shall not be retained in the possession of the Inquiry Officer after a certain amount of time has passed. The 2018 Bill's provision should be restored. Furthermore, the ability of individuals to make copies of confiscated materials should be restored in the current Bill.

36. Clause 62- The Central Government is responsible for determining the number of adjudicating officials to be appointed, the method and duration of their appointment, and the authority of such officers, according to Clause 62 (2). Instead of the Central Government, the Authority should have these powers.

37. Clause 82- The offenses are limited to re-identification and re-identification, as well as the processing of personal data, according to Clause 82 (1). The offenses of collecting, transmitting, or selling personal or sensitive personal data with the purpose or recklessness to do so have been removed.

This section may provide that anytime a data principal's personal data is re-identified or de-identified, the authority performing the procedure shall inform the data principal. Second, we propose the establishment of a new paragraph to allow research exemptions.

Notwithstanding anything stated in subsections (1) and (2), research conducted for re-identification and de-identification following notification of authorities shall be excluded from the foregoing provision,” the proposed subsection 3 should read. As long as the researchers don't reveal or distribute any re-identified or de-identified data without the data principals' permission.

38. Clause 83- Clause 83 (2) states that no court shall take notice of any infraction under this Bill unless the Authority files a complaint. There was no such provision in the 2018 Bill; it just stated that the offenses would be cognizable and non-bailable. It's unclear why such a clause was included in the first place. Prior to the Aadhar Act's 2019 modification, courts may only take notice of a complaint if the Unique Identification Authority of India

filed one. The 2019 amendment altered this, allowing concerned citizens to submit a complaint directly with the court. It's worth noting that this was in response to the Supreme Court's ruling in Puttaswamy in 2018, which said that the Aadhar Act should be modified so that anybody whose rights have been infringed may submit a complaint and start legal action.

This clause should be removed, according to our recommendations. The authority to make a complaint under the Bill should not be limited to the Authority; the affected individual should be able to file a complaint without first approaching the Authority.

39. Clause 85 of the current Bill differs from Clause 85 of the 2018 Bill in that it requires the crime to be “proven” before being found guilty under the Act. When an offence was committed, the provision became effective under the 2018 Bill. The new “prove the offence” criterion is vague and imprecise.

40. Clause 86 empowers the Central Government to provide instructions to the Authority as needed in the interests of India's sovereignty and integrity, security, cordial relations with other states, or public order. Despite the Authority's capacity to voice opinions on any topic, the Central Government's decision - whether to make a policy or not - will be final and binding. In practice, this clause significantly limits the Authority's strength and authority. Given that the binding instructions would concern state security, the provision exposes the scope of exceptions specified in clause 35, as well as the already restricted protections to the same, to possible modification. Human rights may be jeopardized as a result of this.

This clause should be removed.

41. Clause 92- The provision forbids data fiduciaries from processing biometrics that the Central Government may notify them of, unless such processing is authorized by law. It's unclear why such a restriction has been imposed solely on the processing of biometric data and not on the processing of other genetic or sensitive personal data.



This section should be updated to spell clearly the situations in which the federal government may impose a ban on any kind of sensitive personal data, as well as the grounds that will be used to make that decision.

42. Clause 93- This section specifies 25 situations in which the Central Government may issue regulations to carry out the Bili's provisions. We would suggest removing the following from the list:

(a) The techniques of voluntary identification to identify social media users under section 28's sub-clause (3), as well as the identifying mark of verification of a voluntarily verified user under clause 28's sub-clause (4).

(b) A country's entity or class of entities, including international organizations, to whom transfers may be allowed under paragraph (b) of sub-clause (1) of clause 34.

Propose that the following be shifted to the Authority:

(a) Any additional sensitive personal data categories covered by clause 15.

(b) Additional considerations to be considered in accordance with paragraph (d) of sub-clause (3) of section 16.

#### **4.19 INDIA'S HEALTH DATA PROTECTION LEGISLATION**

In India, the health-care sector is booming and evolving at a rapid pace. The patient's personal health information is in the hands of healthcare facilities. The National Health Policy of 2017<sup>94</sup> proposed the creation of a digital health technology ecosystem that would include large-scale data gathering, organization, and exchange.

---

<sup>94</sup>Harleen Kaur and Suresh Kumar Rathi, 'National Health Policies in Practice: An Explorative Analysis for India' (2019) Journal of Health Management 158.

Health data refers to information about the data principal's physical or mental health, including records about the data principal's past, present, or future health, data collected during registration for, or provision of, health services, and data associating the data principal with the provision of specific health services.

The government took the first step in this ecosystem in 2012, when it made it obligatory for clinics to keep electronic health records of their patients under the Clinical Establishment Rules<sup>95</sup>. With the shifting environment, the first concern that comes to mind is the protection of personal and sensitive medical information from disclosure. The issue now is how do we find a balance between security, privacy, and progress.

There is currently no law in India that safeguards healthcare data. The Ministry of Health and Family Welfare proposed 'DISHA' (hence 'Digital Information Security in Healthcare Act') in March 2018, which was the first stage. DISHA is expected to be a law focused on data privacy, confidentiality, and security. DISHA seeks to train administrative experts at the federal and state levels to carry out the rights and responsibilities outlined in the law.

The creation of a National Electronic Health Authority<sup>96</sup> (hence referred to as 'NEHA')” at the federal level was suggested, which would be the highest authority in charge of establishing standards, providing recommendations, and regulating the collecting, organization, and transmission of health data. The State Electronic Health Authority (hereafter referred to as 'SEHA') will be responsible for ensuring that DISHA requirements are met by institutions at the state level.

DISHA is taking a consent-based approach, granting substantial rights to the data owner, allowing him to determine what should and may be done with his personal information. Under the Personal Data Protection Bill 2019 health information falls within the category of 'sensitive personal data. As the name implies, data in this particular category must be handled with

---

<sup>95</sup>Ministry of Health and Family Welfare, 'Clinical Establishments Rules 2012' 5 <<http://clinicalestablishments.gov.in/WriteReadData/386.pdf>>. Accessed on 23 December 2021.

<sup>96</sup> Karl Stoeger and Martina Schmidhuber, 'The Use of Data from Electronic Health Records in Times of a Pandemic-a Legal and Ethical Assessment' (2020) *Journal of Law and the Biosciences* 339.

extreme caution and attention. Under this system, the authorities are obligated to safeguard data, with the main agent having the right to view, delete, and amend personal health information.

Both laws were proposed to safeguard personal healthcare data, but they have yet to be enacted. The reason for this is the growing concern about security as a concept of privacy, which has been established over the last several years. The right to privacy is safeguarded as an essential element of the right to life and personal liberty under Article 21, the Supreme Court said. Furthermore, informational privacy is a subset of it.

The current legal rules governing such protection explicitly state that if a corporate body possesses or maintains any sensitive person information or data and is negligent in maintaining security to safeguard such information or data, a wrongful gain or loss to any individual occurs. And such a body corporate will be liable for damages at that moment. However, the main disadvantage is that it exclusively deals with “corporate entities,” which is insufficient to cover the whole data domain.

Due to the current epidemic of new corona virus (hereafter referred to as "corona virus") the government created the Arogya Setu App, which gives medical information on other individuals, in response to the COVID-19. Along with this, there's the matter of privacy to consider. Many people argue that it breaches the patient's privacy, but if we look at the opposite side, the government is just prioritizing public interest above private interest. According to the Epidemic Diseases Act, the government may take whatever measures are required to stop the illness from spreading, including intruding on people's right to privacy. Furthermore, the law on personal data protection states that in the event of a medical emergency, data protection may be waived without the individual's permission.

#### **4.20 AN OVERVIEW OF HEALTHCARE PRIVACY**

An electronic medical record (EMR)/electronic health record (EHR) is a digitized health record that contains patient demographics, clinical and other treatment-related information in an electronic format. This information is sensitive to the patient and managing them necessitates

preserving the data's privacy and confidentiality. The right to regulate the acquisition, use, and disclosure of one's personal information is known as privacy. The non-disclosure of a patient's electronic health data to undesired and unauthorized individuals is referred to as preserving privacy in healthcare<sup>97</sup>.

One of the advantages of digital health is that it enables for the exchange of health data for better treatment continuity. As a result of this sharing, the danger of privacy is increased. Healthcare professionals are obliged to maintain the confidentiality of healthcare information as part of the ethical duty to first, do no harm, since revealing it may result in extremely severe damage, regardless of whether it is a sensitive topic such as mental or sexual health.

Appropriate rules, data processing procedures, and technological protections may all help to preserve privacy. Threats to privacy in digital health may include:

- Health record theft, loss, damage, or destruction/modification
- Access to health-record systems has been hampered.
- Security and privacy rules are being broken.

The patient, in general, is the proprietor of her medical records. The patient has the right to access her records, to know the facts of her access, and to modify or withdraw her permission. Consent is one of the most important factors in maintaining the privacy and confidentiality of a patient's data. Authorization to conduct healthcare activities, information regarding why, what, and how health information is gathered, and permission for clinical studies are all examples of consent. It also covers the exchange of health data for referrals and research. Patients' or their representatives' permission and access policies should be managed and maintained by each healthcare provider.

The patient has virtually little access to their integrated electronic healthcare records in today's world. As a patient receives therapy from several experts, her clinical, pathology, and imaging

---

<sup>97</sup>Muhammad Anshari, 'Redefining Electronic Health Records (EHR) and Electronic Medical Records (EMR) to Promote Patient Empowerment' (2019) IJID International Journal on Informatics for Development.

data are dispersed across multiple locations. The patient's ability to access the documents is hampered as a result. Due to variations in data quality, interoperability, and interchange due to various applications, platforms, and formats utilized, as well as changes in data quality.

This may be much more difficult in terms of access. The following is a comprehensive list of difficulties in ensuring patient privacy in digital health records:

- Managing the rights of individual participants
- Management of accountability and access
- Data storage and cycle management
- Legal and case management elements
- Privacy rules are applied holistically in both the public and private sectors.

Suppliers of medical services.

- Data transfers across national borders
- Data-control regulatory model
- Breach management, including penalty and punishment management

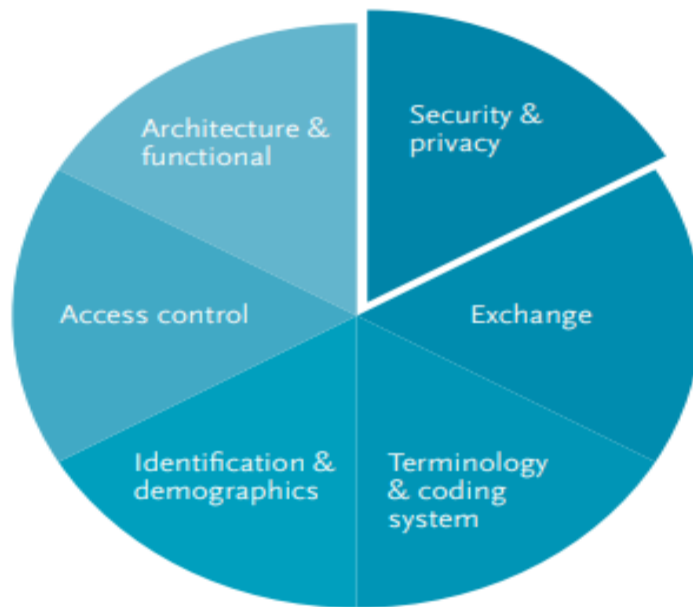
#### 4.21 INDIA'S EHR STANDARDS

India's government wants to create a digital health ecosystem with interoperable electronic health record systems. Only by establishing healthcare IT standards can this be possible. One successful effort, the EHR Standards for India<sup>98</sup>, allows for consistent standard procedures, rules, and processes in healthcare apps. Given that a variety of apps are being used in India's public and commercial hospitals, and that data is being gathered and kept in digital form, the Ministry of Health and Family Welfare issued guidelines in 2016 for the adoption and practice of health IT standards (subsequent to the earlier notification in 2013).

Figure 4.1 shows the suggestions for different areas of healthcare IT/e - Health in the notice.

---

<sup>98</sup>ibid.



*Figure 1: EHR Standards Coverage*

## 4.22 SECURITY AND PRIVACY

The policy, procedural, and technological requirements that assist to guarantee the privacy and confidentiality of electronic health records are all included in the guideline. It specifies the components of medical records that may be considered digitally protected health information (ePHI)<sup>99</sup>. Passwords, financial information, physical, psychological, and behavioral health conditions, sexual orientation, medical records and history, and biometric information are all examples of electronic protected health information (ePHI). For ePHI, the guideline relates to the IT Act of 2000. The following policies must be considered while managing electronic health records, according to the guideline:

### 4.22.1 Ownership of data

<sup>99</sup>Kabelo Given Chuma and Mpho Ngoepe, ‘Security of Electronic Personal Health Information in a Public Hospital in South Africa’ (2021) *Information Security Journal* 67.

The patient owns ePHI, including health information, and the care provider is the custodian of physical and electronic records. A patient may request a copy of her medical records, and health-care providers must disclose all requested information within a certain amount of time.

#### **4.22.2 Data confidentiality and access**

Patients have discretion over who has access to their personally identifiable health information and how it is shared. For access to the information needed for care, explicit permission with an access log must be documented. The patient has the right to request a copy of the whole access log for her medical data.

#### **4.22.3 Information Denial**

On the basis of regular rules and in situations where the information may damage the patient or others, the healthcare practitioner may refuse the information to the patient or any affected/interested person.

#### **4.22.4 Information that is protected or sensitive is disclosed.**

The Medical Council of India (MCI) has established different kinds of consents for treatment, remuneration, non-routine purposes (clinical trials), national priority activities (notifiable illnesses), and so on. Consents are often recorded on papers and kept separately. Consent should be recorded properly in the patient's electronic health records since it is an important component of the health record. The information may also be given without the patient's permission if a court order is presented, and completely anonymized health records can be transmitted by deleting the patient's identifying information.

#### **4.22.5 Preservation of electronic health records**

Individually consolidated electronic health records are clearly a critical source of information for prediction, medical research, and numerous future health revolutions such as personalized medicine, genotype and phenotype-based illness diagnosis, prevention, and therapy. The recommendation advises keeping health records for the rest of a person's life and proposes some methods for dealing with the massive amounts of data being produced.

These recommendations provide a collection of ISO/IEEE-based standards that address elements of healthcare application security, data privacy protection and preservation, encryption methods, storage management, legal considerations, and interoperability standards. Security and privacy, privilege management and access control, audit trails, and general security requirements for health informatics systems are all covered by the ISO/TS 14441, ISO 22600, ISO 27789, and ISO/DIS 27799 standards. The policies and storage methods for maintaining EHR apps are also detailed in the recommendations.

#### **4.23 DIGITAL INFORMATION SECURITY IN HEALTHCARE ACT (DISHA)**

DISHA is the Indian government's strong first step in the lengthy process of safeguarding patient healthcare data in India. DISHA is intended to be a piece of law that focuses on the privacy, confidentiality, security, and standardization of healthcare data. DISHA's main goals are to establish a national and state-level digital health authority, to enforce privacy and security measures for digital health data, and to regulate the storage and interchange of electronic health data.

Although the IT Act's data protection provisions apply to any company that handles sensitive personal data or information (SPDI), the Data Protection Rules' compliance requirements were largely limited to obtaining consent before collecting or transferring SPDI, publishing a privacy policy, and maintaining reasonable security practices and procedures to protect SPDI<sup>100</sup>. There are ISO standards that define the set of criteria that must be met in order to protect a person's privacy. In addition to data privacy regulations, a regulator was needed at both the federal and state levels to enforce the rights and responsibilities outlined in the legislation.

The government has suggested establishing a National Digital Health Authority (NDHA) under DISHA, which would be the lead agency responsible for developing standards, operating guidelines, and procedures for the production, collecting, storage, and transmission of digital health data. At the state level, state digital health authorities will be in charge of ensuring that DISHA's criteria are followed on the ground, at the institutional level.

---

<sup>100</sup> The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011' (n 8) .



DISHA also recommends the creation of e- Health information exchanges, which would process and transfer data across healthcare institutions and serve as the backbone of interoperability and access. Data will move freely between entities as a result of this.

DISHA establishes a broad range of rights for data owners (i.e. patients) and imposes obligations on healthcare data collectors, producers, and processors. The stakeholders' primary duty is to maintain privacy and confidentiality, and any data breach of their digital health data must be reported to the owners.

Data breaches and non-compliance with DISHA's standards are likewise governed by DISHA. In 2017, DISHA was made available for public comment and is now being considered for implementation.

## **CHAPTER- 5**

### **GDPR vs. Personal Data Protection, Bill 2019: justifying the privacy principles.**

#### **5.1 THE EMERGING PILLARS OF DATA PRIVACY LAWS AROUND GLOBE**

Since the previous 18-20 months, we have seen an explosion of data protection laws. 89 percent of the world's population is protected by data protection laws and regulations in some capacity. With the global proliferation of data protection rules, we are seeing is a kind of categorization of various styles or sorts of data protection laws. These laws can be divided into three buckets or pillars<sup>1</sup>. The three global pillars are as follows:

- a) Pillars based on human rights.
- b) Pillars based on damages; and
- c) Pillars based on controls.

##### **5.1.1 Human Rights Based Pillars**

Primary law based on rights is designed after the pillar of the General Data Protection Regulation (GDPR)<sup>2</sup>. This paradigm is founded on rights enshrined in several constitutions, most notably the European constitutional human rights, which states that privacy is a “fundamental right” and that any legislation must respect that right. This is referred to as the privacy pillar.

##### **5.1.2 Harm Based Pillars**

---

<sup>1</sup>Ian Thomas, ‘Getting Ready for the California Consumer Privacy Act: Building on General Data Protection Regulation Preparedness’ (2020) Applied Marketing Analytics 201.

<sup>2</sup> Damian A Tamburri, ‘Design Principles for the General Data Protection Regulation (GDPR): A Formal Concept Analysis and Its Evaluation’ (2020) Information Systems. 74

We can see a damage-based pillar emerging out of North America, namely the United States of America, where the emphasis is on the harm that happens when things go wrong. This kind of pillar is mostly concerned with data breach. What should be done in the case of a breach resulting in damage to people?

### **5.1.3 Control Based Pillar**

The Control-Based Pillar is evident in nations such as China and, maybe, India and Russia, where the underlying law is particularly detailed. The law contains highly specific information about how the legislation should be executed via the use of a set of controls, and the way that privacy model needs to be executed. Based on this concept, other data protection laws have evolved, and several of them are first-time data protection legislation. They are either modelling themselves after one of the pillars, which is often dependent on the geopolitical history of those nations and whomever the economic and political connections establish.

There are certain intriguing provisions in the Middle East that have incorporated elements from all three pillars; thus, it becomes much more a matter of economics and politics as to which pillar such laws fit under.

## **5.2 GLOBAL STUDY**

### **5.2.1 Positions in United State of America:**

In the United States of America, we may see new and domestic legislation forming some of these risk-based frameworks with some of the more rights-based approaches borrowed from nations who have embraced an EU-like sensitivity to this privacy regime.

Within the country, three states have enacted data protection legislation:

- California
- Virginia
- Colorado

Apart from these, there are more states that have laws either in force or in the queue, to be updated in a future legislative session. Some of the concepts outlined in GDPR are beginning to seep into this drafting, coexisting with the previous harms-based approach. For example, California's CCPA has a private right of action specific to data breach incidents, while the entirety of the legislation places a new focus on rights. It's fascinating to see how these growing ideas and pieces of legislation connect in the United States.

### **5.2.2 US and Global Privacy Laws**

Organizations face a continual and everlasting fight, to stay evergreen in a legal framework and environment that is not static. Historically, matching US procedures with those of other foreign regimes was not unheard of since it was an EU mandate in cross-border transfer considerations prior to GDPR. This is not a novel situation for the US organization either. However, it is possible that more robust frameworks must now be examined. Cross-border transfers of data from the EU to other countries have always been a source of contention for global privacy and trade continents. and will continue. For any American organizations lawfully transfer data will be refined and granular now that privacy and the limitations that may arise with standard contractual clauses has been defined. If there are certain constraints on the US National Security stance, what will that mean- is some of the new difficulties that will arise when organizations adjust to developments in that new environment<sup>3</sup>.

### **5.2.3 European Union vs. USA**

If we look at the history of data privacy laws, we can see where it came from. The GDPR, like the preceding EU law, is founded on the Human Rights Charter. If we turn the hands of clock back a little bit, we can see why the human rights charter is

---

<sup>3</sup> Ibrahim Sulieman Al Qatawneh, Wesam Almobaideen and Mohammad Qatawneh, 'A Comparative Study On Surveillance And Privacy Regulations (THE UAE VS. THE USA AND THE EU)' (2022) Journal of Governance and Regulation 32.

considered so sacred in many respects considering the unpleasantness of the second world war and the history of what occurred with nations there and the use of information<sup>4</sup>. Then, before the advent of Google, people used to visit bookstores. These booksellers were the Google of the day; if they needed to find anything, they would go to the bookshop. As a result, bookshops became a location for many individuals who did not agree with the political agenda. Political regimes' political wing and enforcement apparatus would visit the bookstores and request to examine their reader / order list. They used to confiscate the books. There were many persecutions and victimizations based on someone's political opinions, ethnic origin, or religion. These were the events of 80 years ago. This is the context in which the Human Rights Charter was conceived. It was intended to avoid a recurrence of the attribution and was therefore included into one of the European Union's basic human rights. The right to privacy and the right to live successfully undisturbed is one of the fundamental rights of Europe. We can observe similarities in the United States of America as the first and fourth amendments to the constitution. When we look at history, it becomes evident that the American legal system originated from the English legal system, i.e., common law, and then developed its own unique version of it. It stems from the fact that there is a basic human right that must be protected, which may be accomplished via the establishment of a legal framework and supports those fundamental human rights. That is where the directions and eventually the rule controlling the do's and don'ts of personal information processing originated.

The constitution of the United States of America was largely created to protect the public from the government, beginning with the first amendment, which guarantees people's freedom of expression and religion. The fourth amendment, which dates all the way back to the days of ancient English rule, prohibits the government or its agents from entering into the sacred home of the residents of the United States of America.

As a result, although there are similarities to right to privacy, there is no legal right. The Fourth Amendment to the United States Constitution contains an implied right to

---

<sup>4</sup> Nguyen Truong and others, 'Privacy Preservation in Federated Learning: An Insightful Survey from the GDPR Perspective' (2021) Computers and Security 432.

privacy. This is how the various frameworks developed. When there is a discussion regarding “what is right vs. what is harmful”, there is an infringement that the government or another party had violated one of the modifications. This is reflected in the state-level legislation implementing the original data protection rules to a certain degree, in the new legislations of California and other states<sup>5</sup>.

It is critical to understand the historical context in which these regulations and statutes originated. It is possible that the European Union takes a more human rights-based approach to data privacy regulations and regulatory regimes, whereas the United States takes a more consumer protection-oriented approach.

As a result, data protection and privacy are seen to be more of a property right issue. This property right in the United States is the Corporate Property ownership of personal information and the capacity to profit from it, and then balancing that into sector-by-sector ways, for example health care or financial data.

There are distinct rights at stake here, and it has little to do with individual privacy.

#### **5.2.4 Two Pillar Approach**

The approach in the United States is more property-oriented, with a property stake in personal information. This might have an effect on some of the more consumer-friendly policies implemented by the United States on privacy, data protection, and personal data. The United States has not raised privacy to the level of fundamental human rights as that of European Union. The United States has compartmentalized it further by defining it as a property interest, consumer protection interest, and protection against governmental intervention that do not amount to the level of human rights, and raising it to a kind of sacristy level.

#### **5.2.5 Implementation U.S. vs E.U.**

Now, when it comes to organizations, they must examine their worldwide operations and adopt the most stringent approach in certain areas while taking a less stringent approach in others. There are organizations who want to have a globally consistent

---

<sup>5</sup>Thomas (n 1).

strategy. These organizations employ the most rigorous techniques and uniformly apply them. Thus, regardless of whether they are legally required to do so or not, all of their activities will be subject to a strong global data privacy policy.

For example, Microsoft will have a privacy regulation that will apply internationally with minor local adjustments. Both the GDPR and the CCPA ruled out a method that would embrace more stringent requirements going future to ensure that new rules and regulations are included and there is a more evergreen approach<sup>6</sup>. This will not need the constant redesigning of organizations.

### **5.2.6 Privacy Shield between E.U. & U.S.**

The young generation are the ones that pushed Facebook forward. Facebook was mostly responsible for data sharing without consent. Facebook was first brought to task by the Irish Data Protection Commission because it was the lead supervisory authority that existed and operated within the GDPR framework at the time. Under GDPR, any company operating in Europe is required to have a lead supervisory authority and a primary establishment in Europe, which means it should have a legal seat in Europe. The goal is to ensure that the data protection regulator's provision is included in the event of fines. The Irish Data Protection Commission determined that this was an issue too large for them to answer and took it to the European Court of Justice, where it was finally resolved. The initial judgment, which was heavily impacted by the Snowden leaks, ruled that transmitting data from Europe through the privacy safe harbor concept at the time did not provide enough security for such data. The European data transfer model is assertive; it states that the receiving nation should have a data protection level comparable to that of the sending country. The GDPR established a very high bar in 2018 as a result; very few nations met the standards set by the European Commission, dubbed as “the adequacy standard”. The initial court ruling made it quite evident that safe harbor did not provide enough protection in comparison to the scheme. There were

---

<sup>6</sup> Jordan M Blanke, Protection for Inferences Drawn: A Comparison Between the General Data Protection Regulation and the California Consumer Privacy Act (2020) Global Privacy Law Review 13.

other shortcomings, such as self-certification, that prevented it from being monitored as thoroughly as it might have been in accordance with the European requirements.

After a while, a privacy barrier was developed that was stricter and more practical. It performed well when it came to data transmission.

Max Schemes (activist) determined once again that he may take Facebook ahead (Scheme II) on the same grounds that safe harbor was thrown down, namely the alleged disproportionate monitoring of the intelligence community on data sent to the United States of America. It was very contentious and sparked global controversy. This also demonstrates the unfettered nature of European intelligence agencies and the absence of any reference to European surveillance models.

It is important to note that GDPR makes no reference to government surveillance operations since it is covered by a different rule that was prepared concurrently with GDPR. It is a set of rules governing law enforcement intelligence services and data processing (Regulation 680). GDPR was never meant to be applicable to law enforcement.

Schemes II examined the privacy shield in detail. The American surveillance security service is still in force, the European court said, and we are going to repeal the privacy shield as well. It was a complete jumble of what constitutes a legitimate framework for data transfer from the European Union to the United States. There was a model for standard contractual clauses that was quite demanding since it required doing a privacy evaluation of the nation where the data was to be received. This evaluation must be included into these typical contractual provisions.

Why is the national framework not useable

Numerous nations lack data protection regulations; hence, contract law plays a significant role in such countries. It must include all the same protections as a comprehensive data protection legislation, except that it will be enforced under contract law. Legislation governing data protection is enforced through proxy.



Therefore, the privacy shield and safe harbor are still not regarded acceptable methods of data transmission, although contractual provisions are<sup>7</sup>.

## **5.3 CASE STUDY ON CHILDREN’S DATA**

### **5.3.1 UNITED KINGDOM**

The Children's Code, which the United Kingdom's Information Commissioner (ICO) issued in September 2020, was ordered by Section 123(1) of the United Kingdom's 2018 Data Protection Act (U.K. DPA). It consists of 15 criteria for design that are age-appropriate; that any businesses must adopt and apply. By September 2, 2021, any business house that offer online services in the United Kingdom must adhere to the new code of conduct governing the handling of children's personal data, nicknamed the Children's Code<sup>8</sup>.

The Code was developed to adopt a risk-based approach to protecting children's personal data, allowing children to make use of internet services while ensuring that the companies collect and use data appropriately. Business houses should comply with the Data Protection Act of the United Kingdom and the EU General Data Protection Regulation, that govern the processing of children's personal data.

#### **5.3.1.1 To Whom the Code Applies**

The Code applies broadly to online services for a charge — including those sponsored by online advertising — that handles personal data of or are likely to be accessed by children under the age of 18, regardless of whether such services are specifically targeted at minors.

Mobile apps, search engines, social networking platforms, online games and marketplaces, news or educational websites, content streaming services, and online messaging services are all included in this category. Additionally, since the DPA has extraterritorial application in the United Kingdom, the Code will apply to any internet provider — even companies with headquarters in other countries — that provides goods or services in the United Kingdom.

---

<sup>7</sup>Doron S Goldstein and others, ‘Understanding the EU-US Privacy Shield Data Transfer Framework’ (2016) Journal of Internet law 43.

<sup>8</sup>ibid.

### 5.3.1.2 What Services Are Likely to be accessed by Children?

The ICO intended for this term to be widely defined to encompass not just services aimed towards children, but also services that children are "more likely than not" to access, but not all services that children may access.

Considering whether children will be drawn to the type and content of the service, as well as how users may access the service (e.g., if a firm utilises an age gate).

Businesses may make this assessment based on market research, other sources of knowledge about online user behaviour, or the number of users of comparable services.

### 5.3.1.3 The Code's 15 Age-Appropriate Design Standards

Unlike the US children's privacy law, which empowers parents to control the collection, use, and disclosure of their children's data, the UK's Children's Code requires businesses to ensure that data is processed in the children's best interests and that children has the information and tools necessary to exercise control over their data.

The standards of the Code are designed to be technology-neutral design principles that may be applied to a variety of services and technologies. The standards do not limit or define services and will never replace parental supervision and guidance, but will provide parents and guardians greater confidence that their children may safely study, explore, and play online.

- Ensuring that data processing is in the best interests of the child:

This standard reflects the United Kingdom's obligations under the United Nations Convention on the Rights of the Child and requires businesses to prioritize the child's best interests when designing and implementing online services that a child is likely to access. The ICO underlined that this criterion does not exclude firms from pursuing their own financial interests; rather, it requires enterprises to create and implement services that protect children from exploitation and other online harms.

- Conduct data protection impact assessments:

This standard reflects the UK's duties under the United Nations Convention on the Rights of the Child and requires enterprises to put the child's best interests first when creating and executing online services that a child is likely to access. The ICO emphasized that this standard does not exclude businesses from pursuing their own financial goals; rather, it compels them to develop and deploy services that safeguard minors from exploitation and online harms.

- Ensure age-appropriate application of the Code:

Businesses should be aware of the age ranges of children who may use their services to design their services and adhere to the Code in a way that meets the requirements of those children at various ages and stages of development.

- Provide adequate transparency:

Businesses must inform consumers about how they acquire, use, and disclose personal data in succinct, conspicuous, and age-appropriate language. Additionally, businesses should offer just-in-time notification when the data is collected and urge minors to consult with their parent or guardian prior to allowing any additional uses of data.

- Avoid detrimental uses of data:

Businesses must avoid processing children's personal data in ways that are detrimental to their health and well-being. Industry norms, regulatory rules, and other expert assistance should all provide insights into the sorts of processing which are potentially dangerous. The ICO suggests consulting Committee of Advertising Practice advice for information on the types of advertising and marketing that may be harmful to children's physical, mental, or moral development.

- Follow policies and community standards:

Businesses must adhere to their own privacy policies and other public declarations addressing how personal data is handled.

- Develop default settings for high-level privacy protection:

Businesses must establish children's privacy settings to the greatest degree of protection by default, save for the use of personal data required to offer the core service.

- Ensure data minimization:

Businesses may collect and keep no more personal data than is required to offer the components of a service in which a child actively and knowingly participates. Children must be able to choose the components of a service they want to activate independently. This may be performed via the use of the default privacy settings.

- Limit data sharing:

Children's data should be provided only when a company can demonstrate a compelling rationale for doing so, while also considering the child's best interests. Businesses should get assurances from receivers that they will comply with this obligation and do appropriate due diligence to verify that data recipients comply.

- Provide enhanced protection for geolocation information:

Businesses should disable geolocation by default (unless the firm can establish a compelling cause to enable geolocation by default that is in the child's best interests) and offer a clear signal to children when location tracking is engaged. Businesses should guarantee that access to geolocation information is disabled by default once a kid temporarily makes their location available for a specific reason.

- Provide notice of parental controls:

A company that offers parental controls should provide age-appropriate information to the kid about the settings and should make it clear to the child when their parent or guardian is monitoring their online activities.

- Limit profiling:

Businesses should specify options that need profiling to be off by default unless profiling is required to provide the core service. By default, privacy settings governing profiling for online behavioral advertising should be set to "off."

- Avoid the use of nudge techniques:

Businesses should not use persuasive techniques that encourage children to provide unnecessary personal data or reduce their privacy protections.

- Ensure compliance of connected toys and devices:

Businesses that sell connected products, such as linked toys and voice-activated gadgets, must offer adequate means for ensuring compliance with the Code. Devices that may be used by numerous family members, some of whom are children, should be set to provide default child safeguards and user profile choices that allow services to be adjusted to the kid's age.

- Provide online tools:

Businesses must offer easily accessible and usable online tools that enable children to exercise their rights and raise concerns.

### **5.3.2 CANADA**

Consent that is meaningful is a critical component of Canadian private sector privacy regulation. Organizations are typically obliged by privacy regulations to get meaningful permission before collecting, using, or disclosing personal information. However, technological advancements and the proliferation of long, legalistic privacy regulations have all too often rendered the control – and personal liberty – that consent should permit illusory. While consent should remain fundamental, it is vital to reimagine how it is received.

Children and adolescents' capacity to provide meaningful permission to the sharing of their personal information is highly dependent on their cognitive and emotional

development. Given the difficulty adults have comprehending what happens to their personal information in a complex environment, it would be absurd to expect youngsters to completely comprehend the intricacies and possible hazards associated with sharing their personal information. Private sector privacy regulation recognizes this by allowing permission via an authorized person, such as a parent or legal guardian.

We acknowledge that the maturation process is dynamic, as youngsters become more exposed to – and consequently gain an awareness of – information-based services at an earlier age. While a child's competence to consent varies by person, the OPC believes that there is a threshold age below which young children are unlikely to completely comprehend the implications of their privacy decisions, especially in this era of sophisticated data flows. On the other hand, the OIPC-Alberta, the OIPC-British Columbia, and the Quebec CAI do not specify an age limit, but rather assess whether the person understands the nature and implications of the right or authority in issue. As such, when a child is unable to agree meaningfully to the acquisition, use, or disclosure of personal information, The OPC maintains that, unless in extraordinary situations, anybody under the age of 13 must get agreement from their parents or guardians<sup>9</sup>. For children capable of providing meaningful permission, consent may be regarded meaningful only if organizations developed and updated their consent procedures with due regard to their maturity level. Organizations collecting, using, or disclosing such information should exercise great caution to maintain accountability and be prepared to show on demand that their chosen approach results in meaningful and valid consent.

#### **5.4 ASIA PACIFIC PRIVACY REGIME**

As previously stated in this chapter, the Global Privacy Regime represents a significant schism between the United States of America and the European Union. It is critical to monitor the situation in the Asia Pacific area to get further clarification on privacy principle and harmonization.

---

<sup>9</sup>Timothy Banks, 'GDPR Matchup: Canada's Personal Information Protection and Electronic Documents Act' (2017) The International Association of Privacy Professionals.

The most critical part of privacy regulations is their harmonization and interoperability. We can appreciate this by looking at the World Bank, which is hardly a stronghold of data protection. The 2017 Globe Development Report titled Digital Dividends emphasized the ongoing need for uniform, dependable data protection legislation as a critical aspect in decreasing inefficiencies and encouraging consumer confidence around the world. As we can see, any regulatory structure that is incompatible with the flow of business information incurs huge costs and inconveniences. The issue now is where this regular, dependable control is located. Is it the OECD, the GDPR, or the APEC guidelines, for example?<sup>10</sup>

Each of them has merits and demerits, but none forms international law exactly as a formal treaty does. There is a significant legal void in international law because of the absence of a framework convention on data privacy legislation.

A treaty as a legally enforceable duty must be formulated with the following standards:

- a) Maintaining the country's reputation for adhering to domestic human rights protections and privacy laws.
- b) Maintaining the country's reputation for adhering to domestic privacy rules.
- c) A dedication to human rights on a broad scale.
- d) Adequate data protection requirements must be provided.

#### **5.4.1 NEW ZEALAND**

It is necessary to emphasize that data privacy regulation is evolving year after year. While New Zealand's data privacy legislation was being written, analogous transactions occurred in the European Union<sup>11</sup>. The European Commission was in the process of finishing preparations for the GDPR's implementation. On the other hand, the New

---

<sup>10</sup>Md Toriqlul Islam, Mariyam Sahula and Mohammad Ershadul Karim, 'Understanding Gdpr: Its Legal Implications And Relevance To South Asian Privacy Regimes' (2022) UUM Journal of Legal Studies.

<sup>11</sup> Jonathan Barrett and Luke Strongman, 'The Internet, the Law, and Privacy in New Zealand: Dignity with Liberty?' (2012) International Journal of Communication 232.

Zealand government was adopting recommendations by the country's law commission about privacy law reform. The Council of Europe was discussing modernization, while New Zealand's data privacy legislation improvements moved it closer to the GDPR, but not as near as it might have been. After minor revisions/amendments, New Zealand's legislation became effective in July 2020 as the Privacy Act 2020. The following are the salient features of New Zealand law:

- a) Mandatory breach reporting
- b) Robust enforcement capabilities
- c) Restrictions on data transfers that are transported

Though a strong regulation, the law falls short on several issues, including:

- a) Rights to object to automated data processing.
- b) Mandatory "privacy impact assessments; and
- c) Defining special categories of personal data. While New Zealand's law provides a comprehensive standard of protection for individuals' rights, it falls short of GDPR's breadth.

#### **5.4.2 AUSTRALIA**

Australia is currently reviewing its privacy laws. There is a well-established privacy framework in place that incorporates references to both the OECD's recommendations and the international covenant on civil and political rights. It is founded on principles and is both neutral and adaptable in terms of size and breadth<sup>12</sup>.

#### **5.4.3 PEOPLE'S REPUBLIC OF CHINA**

---

<sup>12</sup>Angela Daly, 'Privacy in Automation: An Appraisal of the Emerging Australian Approach' (2017) Computer Law and Security Review 505.



On August 22, 2019, the China Cyberspace Administration (CAC) published a new data privacy rule affecting children, the Provisions on Cyber Protection of Children's Personal Information (PCPPIC)<sup>13</sup>. The rule takes effect on October 1, 2019 and is applicable across the People's Republic of China (PRC). The stated aim of the PCPPIC is to protect children's personal information and encourage their healthy development in the PRC. The PCPPIC has 29 articles outlining high-level standards for the collection, storage, use, transfer, and disclosure of children's personal information inside PRC territory.

#### 5.4.3.1 Defined Purpose and Parental Consent

The CAC mandates that network operators collect, utilise, and keep personal data in compliance with the criteria of righteousness, necessity, informed consent, particular purpose, security assurance, and its authorised use. Personal information must be handled in a manner consistent with the business services given to minor users. Data should be retained for no longer than is required to fulfil the agreed-upon objective and scope of the business service.

Children are defined under the PCPPIC as minors under the age of 14<sup>14</sup>. Prior to collecting or using children's personal information, parental or guardian agreement must be acquired. Additionally, network providers must include an opt-out mechanism. Network operators must offer information on the following six areas when getting consent:

- The purpose, scope, method, and duration of data collection, storage, use, transfer, and disclosure
- The location and treatment of data after the agreed term expires
- The security measures in place to protect data
- The consequences of a parent or guardian refusing to provide consent
- A mechanism for parents or guardians to report violations or file complaints with the network operator regarding the mishandling of children's personal information

---

<sup>13</sup>Noval (n 16).

<sup>14</sup>Lothar Determann and others, 'Practice Papers China's Draft Personal Information Protection Law' (2021) Journal of Data Protection and Privacy 88.

If any changes take place in the above mentioned points, network operators are obliged to re-obtain parental or guardian agreement.

#### 5.4.3.2 Information Security and Third-Party Considerations

Network operators are obliged to establish special policies and procedures for the protection of children's personal information, as well as to enter into a contract with users. Network operators should take reasonable steps to protect information by encrypting it or using other acceptable means. Network operators are obligated to provide rigorous access permissions for people responsible for handling children's personal information in accordance with the idea of minimal authorization.

Prior to transferring personal information to third-party suppliers, network operators are obliged to complete a security evaluation of the transferee. Additionally, network operators should sign into entrustment agreements with third parties to establish their respective obligations, the type, purpose, scope, and duration of data processing.

Children or their parents/guardians have the right to seek adjustments to or deletions of their children's personal information and network providers are required to comply with such requests under the PCPPIC. If a child's personal information is disclosed, destroyed, or lost, network operators must promptly notify the parent or guardian and take corrective action.

### **5.5 Notable Differences among the PCPPIC, COPPA, and the GDPR**

#### *5.5.1 Jurisdictional Age Gate*

The Children's Online Privacy Protection Act (COPPA), the US federal statute that is equivalent, has been in effect since 1998. Twenty years later, in May 2018, the EU implemented an article 8 of the General Data Protection Policy (GDPR)-related data privacy regulation for minors (GDPR). As it is with COPPA and the GDPR, the PCPPIC outlines parental/guardian permission requirements and the network operator to protect the privacy of the children's data. All three bodies of legislation require that the collection and use of children's personal information be limited to the narrow extent needed by the business service, with parental/guardian agreement

that is legal, informed, and voluntary. One major distinction between the three bodies of law is the jurisdictional threshold age for minors. The COPPA sets the consent age at 13, whereas the GDPR sets it at 16. (With the provision that Member States may adopt even younger markers, as low as 13). In comparison, the PCPPIC age restriction is 14.

### 5.5.2 Jurisdictional Reach

Another significant distinction is that COPPA applies widely to any online service, regardless of its place of origin, if it is aimed at US residents. Therefore, COPPA protects minors even if the network operator is situated in the United States. In contrast, the GDPR concentrates on the geographic location of children and applies solely to businesses that collect and store personal data of EU residents, regardless of the company's location. Similarly, to the GDPR, the PCPPIC relates to minors within the PRC's territorial jurisdiction and makes no mention of extraterritorial effects<sup>15</sup>.

### 5.5.3 Penalties

The PCPPIC imposes punishments in general. Article 26 says plainly that violators of the PCPPIC would face penalties under applicable laws and regulations as established by the CAC and other appropriate government authorities (e.g., the People's Republic of China's Cyber Security Law). By contrast, the COPPA and the GDPR both have very precise sanctions. Operators that violate COPPA may face civil fines up to US\$42,530 for each infraction. When determining fines in the United States, a court will consider the gravity of the crimes, any past violations, the number of minors involved, and the quantity, kind, and use of personal information acquired, among other criteria. The GDPR imposes administrative penalties of up to €10 million for breaches of Article 8, or up to 2% of the network operator's prior financial year's total global annual revenue, whichever is greater. In contrast, the PCPPIC makes no explicit provision for maximum sanctions.

---

<sup>15</sup>Natalija Vljajic and others, *Online Tracking of Kids and Teens by Means of Invisible Images: COPPA vs. GDPR*, *Proceedings of the ACM Conference on Computer and Communications Security* (2018).

## **5.6 Children's privacy under the Indian Personal Data Protection Bill 2019.**

The Clause that directly deals with Personal Data of Children.

The Protection of Children's data can be seen under 2 key concepts:

1. Data of Children
2. Data from Children

With the introduction of fertility and parenting applications, data collecting on children starts even before the kid is born. Parents begin by entering information on their unborn kid, followed by new-born and babies<sup>16</sup>.

Similarly, schools retain sensitive personal data about all pupils on digital platforms beginning with the minute a parent completes an entrance form. In these instances, children are not the data principals, and data management decisions are made by the guardians and data fiduciaries concerned<sup>17</sup>.

When it comes to collecting data from children, it is often initiated via their interaction with online games, media, and educational tools. This is when the notion of permission enters the picture. Because in this scenario, data subjects (children) are active participants in the data gathering process.

The age of consent is raised in this instance.

The suggested consent age of was 18 years in the 2019. The draught law was not determined on the basis of fair rationale, given the contemporary reality of the internet and its pervasiveness.

The current draft of 2019 views consent as a contract and hence follows the existing contract law in establishing the required age for consent. However, given that the current generation of children in the information age has unprecedented access to global knowledge, law should be written in such a way that it encourages responsible internet usage, even by youngsters.

---

<sup>16</sup>Purushotham Kittane and others, 'India Privacy and Data Protection 2020 Wrap' [2021] National Law Review.

<sup>17</sup>Diana Lee, Gabe Maldoff and Kurt Wimmer, 'Comparison: Indian Personal Data Protection Bill 2019 vs. GDPR' (2020)IAPP.

Additionally, the regulation must correspond to worldwide standards such as the General Data Protection Regulation (GDPR). While the GDPR stipulates a minimum age of 13 years for acquiring a child's valid consent and a maximum age of 16 years. However, the PDP, Bill 2019 does not allow for such flexibility.

While determining the appropriate age for giving legal permission, many factors needed to be considered, including the following: - a) From the developmental psychology perspective, a kid at the age of 6 or 7 years is not the same as one at the age of 14 years and should not be viewed as such.

b) From a parity perspective, equitable access to modern technology continues to be a distant dream in India, particularly in rural India. There is a divide between urban and rural children's access to the Internet; there is a divide between men and women; there is a divide between the higher and lower income classes; there is a divide between upper caste and lower caste households. Children from educated and upper-class families will have more access to internet services that meet global standards under the existing structure. Because their guardians will be enabled to utilize online tools and examine the advantages of children being online, enabling them to make educated choices on their children's behalf.

Children from marginalized backgrounds, on the other hand, will be surrounded by consenting adults who are empowered to make educated choices. In this situation, gaining agreement from guardians will disfavor a subset of the population.

This setback was exacerbated further by Covid's expanded internet presence.

c. Consideration should also be given to the security of children's data<sup>18</sup>. The designation of data fiduciaries who handle children's data as guardian data fiduciaries is critical in this context because it emphasizes the necessity for additional precautions. However, the laws pertaining to the processing of children's data by guardian data fiduciaries should be interpreted positively rather than restrictively in terms of "harm prevention."

---

<sup>18</sup>Graham Greenleaf, 'India's Personal Data Protection Bill, 2019 Needs Closer Adherence to Global Standards (Submission to Joint Committee, Parliament of India)' [2020] SSRN Electronic Journal 78.

Guardian data fiduciaries should be required to take all reasonable precautions to secure children's data and to simplify data processing procedures for consent givers.

d. The current structure must be made more adaptable to the reality of not just the elites and urban upper middle class, but also of the common Indian, who views data differently.

### **5.7 United Nation Convention on Rights of Child**

Article 16: It refers to a child's right to be free from arbitrary or illegal intrusions into his or her private, family, home, or communication, as well as from unlawful assaults on one's honor and reputation.

Additionally, this agreement establishes guiding principles such as non-discrimination and acting in the best interests of the child.<sup>19</sup> These are fundamental notions that have arisen throughout the process of developing any rule pertaining to children.

Another key element is the children's right to education and access to digital literature.

While the permission that results from this worldwide legislative framework is critical for the privacy of children, there are other considerations that must be considered.

### **5.8 Indian Threshold**

In the Indian setting, we continue to depend on traditional concepts of consent when engaging into contracts or sexual encounters. For instance, in India, the criminal justice system acknowledges that minors attain a certain degree of maturity and may be punished on a sliding scale between the ages of 13 and 18. While criminal law also employs a phased strategy to treatment of children depending on their psychological and mental maturity level. After the age of 14, children may also engage in dangerous occupations of their own will under labor law. Indian data protection regulations should

---

<sup>19</sup>Fegert (n 20).

likewise use a similar staggered approach. If the age barrier is not altered, it will have a significant influence on young individuals' overall development.

## **5.9 DATA PROTECTION BILL CASE STUDIES**

The rationale for considering children and everyone under the age of 18 is because they make up almost 39% of India's population. Naturally, they also form the country's most active internet user base. They are vulnerable and hence need protection. However, it is necessary to safeguard their right to privacy, speech and expression while protecting them.

After two years of deliberation, the joint parliamentary committee, abbreviated as JPC, issued its report on the personal data protection law 2019 on December 16, 2021. This paper summarizes the JPC's proposals for amending the personal data protection law 2019 and its provisions on the processing of data pertaining to minors. JPC's suggestions also include privacy for minors under the age of 18 and constructive rules or standards of practice.

The data protection legislation includes specific dos and don'ts for organizations that gather any form of personal data. It advocates for a holistic approach to privacy in terms of design and strategy. There are privacy policies that govern the acquisition of data, what it should include, how permission is obtained, and other transparency measures; all of these standards continue to apply when data about children is gathered and utilized. The law recognizes that children are a particularly vulnerable segment of society and hence need special protection. The legislation establishes extra do's and don'ts for organizations that handle, acquire, and use such data.

The first of the two criteria is that before an organization processes a child's data, it must verify the child's age and get consent from the child's parents or guardians.

A few items to unpack

1. How the law defines a child - Anyone under the age of 18 is considered a minor. The bill opts for the age of majority as defined by Indian Contract Act, which states that an individual may enter into a contract legitimately at the age of 18. Therefore, the first step for any website, App, or online service would be to authenticate an individual's age prior to collecting any of their

personal information. If a person is under the age of 18, his or her data cannot be collected unless the individual's parents/guardians agree to the collection.

This applies to all organizations, regardless of whether they are geared towards children or not. Even if it is a news website that enables users to subscribe to monthly or daily newsletters by entering their name and email address, there is some form of check box or confirmation that the user is above the age of 18.

Regulators are free to choose the specific mechanism of age gating. According to the legislation, age gating should be determined by the risk of damage to a person and the potential of collecting or processing children's data. Some examples of how this type of age verification might look at are - a simple self-confirmation or check boxes where the user checks a box that says 'I am 18', or in the middle of a form, the user enters his or her date of birth and is directed to a platform where he or she must obtain parental or guardian consent. It is not specified in depth in the legislation.

A news website may provide a different amount of risk to a person than a dating app, which may pose a greater risk to a child's privacy. Regulators are yet to determine the kind of confirmation or age gating mechanism that will function. The way in which this permission is granted is not specified in the legislation. It is probably difficult to detail how this will function comprehensively. Other methods of obtaining parental consent may be used, such as asking the child or individual to enter their parent's phone number or email address for OTP verification, or it may be a knowledge-based authentication, such as quizzes or questions that only an adult can answer, or a call center-based verification, such as sending a toll-free number for parents to call and confirm, or it may be an AI-based verification.

These may not be foolproof. Children today have their own phones and may be able to answer certain GK questions more accurately than an adult; call-based verification may add significant friction to the process; official ids or AI-based verification will need more data processing.

It's expected that a law or codes of practice, and regulations will emerge on account of this friction. Perhaps there will be a risk-based spectrum of options presented for example, an age verification for a 17-year-old subscribing to a newsletter will be quite different from an age



verification of a 9-year-old attempting to enter a dating app. This is first assessment of what should be done prior to processing or collecting the child's data.

2. When an organization collects and processes data on a child, the law states that the organization cannot profile, track, or behaviorally monitor the child, or present targeted advertisements to him/her, or engage in any other activity that might cause the child significant harm. There are various advantages of predictive profiling like techniques for determining the kind of interventions necessary for a vulnerable youngster. A school or an edtech platform may create exams and quizzes based on a child's prior performance, which also involves profiling. The legislation does have an exemption for when a youngster cancels services. It is meant to prohibit profiling that might result in serious damage to a child and is not useful at all.

There are additional requirements for processing a child's data in a way that safeguards his or her rights. The frame here is one of a child's rights that is in the child's best interest.

If an organization provides a service to a child or processes children's data, it is designated as a data fiduciary, and must register itself with the authority to conduct data protection impact assessments prior to engaging in any high-risk profiling or processing activity. Periodic audits for these organizations are also required.

The following are the changes between the current and previous versions of the bill: -

1. The concept of best interest has been altered. It now relates to the child's rights.
2. In the previous version of the law, the idea of guardian data fiduciaries was limited to minors and organizations that handled substantial amount of children's data. They were prohibited from profiling, tracking, and similar activities; now, all data fiduciaries face the same prohibition.
3. Additionally, the committee suggests that the government should establish laws allowing individuals who reach the age of 18 to browse websites without the consent of their guardian. The JPC leaves to the government in developing and enforcing regulations on this subject.

A few points to recap and maybe give some contrast

1. Child's age – Many stakeholders believe that 18 is an inappropriate age for parental consent. Allowing parents to monitor a child's every move, particularly in situations where a child may

come from an abusive household or may be looking for information about sexual orientation or other topics that are taboo in their homes is not in the best interest of the child. In the United States, for example, the COPPA (Children's Online Protection Act) defines a child as 13 years old for websites and online services that need parental approval. In Europe, minors only between the ages of 13 and 16 need parental permission to visit internet sites.

These nations also define the types of platforms that need parental approval. In other jurisdictions, the platform seems to be defined more narrowly. Only if a website or online service is oriented towards minors and there is a possibility of damage being caused to a child only then a parental consent is needed. In comparison, Indian law requires all web platforms that engage with any person to have age gating system. Other jurisdictions either permit it with parental approval or prohibit it under certain circumstances and situations. While there is no absolute restriction in Europe, the organization must do impact assessments, adhere to all the privacy design principles, and ensure that the privacy of children is protected at every level of the process.

A poll of 1200 parents and young people was performed to ascertain their perspectives about safeguarding children's personal data under the personal data protection law. The participants were users of digital-driven technology from all around the nation, including young people between the ages of 16 and 17, as well as parents. The diverse group comprised of individuals of mixed gender, geographical location, and educational attainment.

The outcome was astounding.

Numerous young users use a variety of popular data-driven web services without their parents' knowledge. A significant proportion of parents were unconcerned about their child using services without their consent. Additionally, parents assert that children begin using internet-enabled gadgets without parental supervision as early as the age of 14. As a result, the DPB recommends revisiting the age of 18 years for parental approval to browse a website. It would be preferable if we conducted a stakeholder engagement prior to establishing a lower age criterion, as has been done in other nations such as the United States and the European Union.

Children's perspectives should also be considered. Oftentimes, youngsters between the ages of 16 and 18 do not want to agree to many things from their parents. It is not true that everything

the youngsters attempt and accomplish is incorrect. While there are certain things children do incorrectly on the internet, there are also other things that are necessary for their development, and many parents are not as open as they should be, which results in children requesting information about them online. Undoubtedly there are concerns, but they must be addressed.

Then, under clause 162, data fiduciaries are required to get parental permission before processing the children's data. However, it was shown that most parents feel that their children are more knowledgeable than they are about the procedures to follow for a safe internet experience. Additionally, they regard minors to be competent of consenting to the terms and conditions of service providers, an assertion that is backed up by young adults. Separately, most teenage users do not want their internet conduct monitored by their parents. They assert that they respect privacy from all parties, including service providers and the government, as well as their friends and even their parents. As a result, it is required to reconsider the obligation for service providers to seek mandatory parental agreement for services, particularly about young people, defined as individuals aged 16 to 17 years of age.

Numerous young users endure a variety of negative experiences online, including cyber bullying, cyber staking, and so on. While most of them claim to be aware of numerous tools and tactics for overcoming negative experiences, the reality is that many do not use them. As a result, the government and service providers must collaborate with consumer and children advocacy organizations to promote awareness and capability for "safe" internet engagement for children. It remains to be seen, if the data protection law is the appropriate legislation to solve this problem.

Finally, clause 165 prohibits service providers from profiling, tracking, or monitoring children's behavioral attitudes. Most parents and children are okay with service providers adopting various steps to provide a secure online experience, including tracking and monitoring their children's online behavior. Additionally, they wish to employ technology to determine a user's age rather than connecting an ID card. This must be limited to maintaining a secure internet experience for children and not for any other reason. According to child psychiatrists, there may be a need to encourage service providers that monitor children's online activities with specific precautions in place, such as purpose restriction, data reduction, and so on. Additionally, it was discovered that parents and young users prefer to utilize technology to determine a user's age rather than

attaching it to an ID. Under clauses 163 and 56h, the DPB may establish suitable norms of practice for age verification techniques.

While hearing the Aadhaar issue, the Supreme Court was confronted with the problem of how to measure privacy, necessitating a referral to a bigger court. The Supreme Court's nine-judge bench unanimously declared that the Right to privacy is a fundamental right guaranteed by Article 21 of the Indian Constitution. Subsequently, as the Aadhaar dispute advanced, the Supreme Court remarked in its verdict that the government should really enact laws to safeguard people' personal data<sup>20</sup>. As a result, the government established a committee chaired by Justice Sri Krishna. The committee recommended changes and attached a model law. Subsequently, the government produced its own version of the personal data protection law, which significantly varied from the one proposed by Justice Sri Krishna. Parliament submitted the bill to a joint committee of both chambers known as the JCP (Joint Committee of Parliament). Unfortunately, when the bill was brought before the committee, the country was struck by the first instalment of pandemic COVID-19, and after a short two or three sessions, the committee was forced to disband due to the national lockdown. While the first wave was raging and there was no vaccine available, the Committee met from July to December 2020 to go through the law, clause by clause. Before the dawn of 2021, the committee engaged in extensive deliberations for around seven months, but there was no trace of the committee's report being disseminated to members<sup>21</sup>. This was followed by a cabinet change, with the then-chairperson being replaced by a new chairperson, who then reviewed the committee's work. With his wisdom, the new chairperson proposed a set of revisions to the proposal that was left frozen in December 2020. The positive outcome was that it provided enough opportunity to reflect on the Committee's work. The Committee found that the DPB was completely faulty and so rejected the bill in its entirety, as well as the rationale for its rejection. They contended that the DPB divided the country into two distinct sectors: private and governmental. While the law is to be strictly implemented in the private sector, it is replete with exception provisions and blanket exemptions under terms of Section 12 and Section 35 of the bill. A fundamental right is primarily enforceable against the state; it is not enforceable against private entities to the same extent. Therefore, if the right to

---

<sup>20</sup>Ajay S Ghangare and Anup R Ranade, 'Aadhaar Card – Perspectives on Privacy' (2019) *Journal of International Pharmaceutical Research* 343.

<sup>21</sup>Dvara Research, 'Comments to the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill 2019 Introduced in the Lok Sabha on 11 December 2019' (2020) *SSRN Electronic Journal* 78.

privacy was the synagogue of the entire data protection bill, there would be no scope or wiggle room for having clauses exempting the government from the bill's provisions lock, stock, and barrel.

Unfortunately, this basic problem in the bill's drafting called into doubt the bill's legality. The law has an impact on federal-state relations; in other words, the measure is a piece of central legislation staffed by central government officials. Having superintendents and jurisdiction over data by the central government which is within the purview of state governments under Article 246 and Schedule 7 of the Indian Constitution would result in significant issues with this law<sup>22</sup>.

Insofar as the specific subject of discussion, where the age of consent of a child, is concerned, the committee deliberated on it for an extended period and concluded that a blanket determination of a child's age does not do justice to the digital universe in which we live. It's a total oxymoron that a young adult of 13 to 14 years of age must get parental approval every time he attempts to surf the internet or access a website. Subjecting young children to this kind of provision will really create a world of deception and dualism. In terms of the data protection authority, it will be an overburdened entity that will be completely overwhelmed by the sheer volume of work required of it because of the million and millions of data fiduciaries. A large portion of this bill is completely unworkable because of the cost of compliance. The expense of compliance for smaller firms is likely to be so high that it will destroy the country's startup economy.

The bill's structure gives the government an absolute veto. The bill's section 87 specifies that the data protection authorities must follow the directives. It also states that the government will define the public policy and that the data protection authority will be obligated to implement it. In other words, the DPA would be constrained not just by policy considerations but also by the instructions of the government. The DPA really goes beyond the restricted scope of policy, basically stating that the government will choose what the DPA will do or not do, thereby removing the regulator's independence, which will withstand judicial examination. Verification is a difficult problem, and the committee has spent some time contemplating how this verification system would operate. Until the user submits government-issued identification, it

---

<sup>22</sup>Abu Bakar Munir and Siti Hajar Mohd Yasin, 'The Personal Data (Protection) Bill 2009' (2010) *Malayan Law Journal* 87.

will be unable to indemnify the data fiduciary to some degree<sup>23</sup>. If the user submits a fraudulent Aadhar card or a faked school id, it is illogical to expect the data fiduciary to be liable. Thus, this is a total and utter minefield; it should be a graded concept with some of the space entirely free, such as a learning website. While many sites should be totally free from age-verification, others may need some type of verification to safeguard the child and his/her personal data, which is the true purpose of the law.

The bill is no longer a law protecting the personal data but also the non-personal data. In terms of deleting the clause based on the child's best interests, was ambiguous and vague. Who has the authority to decide what is really in a child's best interests – is a million-dollar issue? There are cultural and regional sensitivities; some things may be acceptable in one section of the nation but are considered taboo in another. As a huge nation with varied social patterns and cultures, India's whole digital environment is immensely concerning.

If one must say, we are indeed living in a forest of wickedness, and the anonymity afforded by social media has enabled the society's darkest inclinations to reveal them in public space. As a result, the data protection authorities have their hands full. This measure establishes some fundamental ideas, but when put to the test and dissected, they will undoubtedly prove to be a nightmare.

Does it really stand up to the "right to privacy judgment," a nine-judge bench decision of the Supreme Court? The measure in its present form may be deemed unconstitutional, which is one issue that the administration is unwilling to examine. There has been much discussion about Sections 35 and 12 of the DPB, which provide for the government's breakout or escape provisions, but the government is unwilling to relinquish even a single inch, and therefore there is a long road ahead of this bill's enactment.

There are two major issues with the bill's construction. The first is that the fundamental rights asserted before constitutional tribunals under Articles 32 and 226 are fundamentally anti-state. Thus, the Supreme Court's view in the Puttaswamy Case<sup>24</sup>, by including informational privacy as a component of the right to life under Article 21, effectively guarantees citizens this right under

---

<sup>23</sup>ibid.

<sup>24</sup>Mariyam Kamil, Puttaswamy: Jury Still out on Some Privacy Concerns? (2017) Indian Law Review 90.

the constitution. The bill's passage will drive individuals to the courts to vindicate their rights against the state, which may be the central government, the state, or any of the state's agencies. As a result, the central government will choose how the law is to be phrased at each location and in each part. Indeed, so many issues have been delegated to the central government that, if they so want, they may amend the law by executive orders. This would imply that the bill's overall structure is insecure and unpredictable.

The second component of the bill, which is also a structural issue, is that many of the country's legislations classified as state legislation are enacted via state. Because when the data is gathered by state agencies, there is no legal or practical reason to assign adjudication of these concerns to a central body that would almost certainly designate many of its personnel in states as adjudicators. It is like having the income tax, customs, or enforcement department. At least two states performed the same thing during the committee's state visits and field tours. The committee most likely erred by failing to include the state government during its primary consultations, as it should have done, which explains why there are issues with the bill's structural architecture as it now stands.

Thirdly, DPA would be overwhelmed by the scope of work required for the bill's amendment. Apart from the legislation, the code of practice, and many interactions with sectorial regulators, the task will be quite difficult. Harmonization of the many acts and different laws in effect that authorize a certain body to gather data would be difficult. The present bill has chosen the simpler route by declaring that everything enacted by parliament is law, allowing data to be acquired beyond the scope or authority of this bill. Even if it is subsequently contested in court, it will have less legal significance than in other countries since this specific right has been recognized as a basic right. It has not been recognized as a basic right of people in other countries.

Concerning problems of privacy and minors' rights, the OECD's (Organization for Economic Co-operation and Development)<sup>25</sup> risk typology states that the internet risk from a consumer viewpoint is a privacy and security risk. While this law addresses privacy and security concerns, it does not address the internet and consumer risks that a youngster would encounter. And although those hazards are likely addressed in separate laws. All three of these pieces of

---

<sup>25</sup>Fateh Habibi and Mohamad Amjad Zabardast, 'Digitalization, Education and Economic Growth: A Comparative Analysis of Middle East and OECD Countries' [2020] *Technology in Society*.

legislation like CRPC, IPC, IT Act etc must coexist and coordinated. Therefore, when they set the age of 18 years for a child to become an adult in accordance with the Contract Act, this law may have benefited from a clause allowing for graduated age discrimination or an age verification exercise. The young men who are either digital naive or digitally informed have a reasonable understanding of how parents' consent is done on their child's behalf to allow access to the internet or services provided by data fiduciaries. One must also take into account the geographical and cultural differences across the country. While implementing this rule, the DPA would not have an easy time balancing the interests of children and privacy. The advantages that should accrue to children because of using the internet, different services and applications, and anything else should be made accessible to them even without their parents' approval, since many parents are unaware of the benefits that will accrue as a result of internet usage. There is also a substantial amount of data about children that is maintained manually. There is an omnibus clause in the bill that allows for an exception but whether an omnibus exemption for data held manually on minors and at schools and colleges located in rural and distant places is appropriate or if it should be covered by the act is a huge concern. Now, there are certain operational concerns that might arise because of ageing. Indeed, if a state-level data protection authority had been established, several of these concerns pertaining to regional and cultural diversity might have been handled considerably more effectively than via a central or monolithic agency, as the law presently envisions<sup>26</sup>.

On the one hand, permission is critical; on the other hand, even if parents agree to their children's data being gathered by a data fiduciary, there should be a mechanism for removing guardian data; otherwise, there would be no data that is entirely of children. Children's and guardians' data sets will certainly be intermingled. As a result, any data fiduciary who handles this kind of data would be susceptible to this. Even after obtaining parental approval, the chance of damage occurring inadvertently or purposefully exists; yet just because consent has been obtained, the data fiduciary will not be held accountable. Thus, a harm-based approach would have been much more suited in the instance of children's data. We still have time to have it in the shape of regulations and rules. The penalty for dealing with children's data in a completely different context, namely for child pornography and generation propagation which should be severe. The

---

<sup>26</sup>Rajat Misra and Rajat Grover, 'Future of Privacy: Evaluating the Personal Data Protection Bill, 2019 in Light of Contract for the Web' (2020) SSRN Electronic Journal 63.



DPA and government must work on aligning the illegality of such actions between this law and the CRPC, IPC, and the IT Act. As circumstances change, the law should adapt to the changed circumstances and be recorded. Since legislation constantly lags the progress in technology. It would be better if the technology could identify a child from an adult and use documents like an Aadhar card or a school id whichever is adequate and no other physical information is required. Let technology tackle the issues without the law getting much involved<sup>27</sup>.

An age-related problem is also there when a minor wishes to get a SIM card. He is not permitted without the permission from his parents or guardians. That is why the debate over a mandatory minimum age of 18 years was undertaken. If a balance is struck between the advantages that a youngster may have, the missed opportunities, and the child's privacy, this age is appropriate. Currently, the law is set in stone and may be brought to the Parliament sometime in future to implement a graduated age verification system. It may be difficult at this stage, but the rules could come in to explain and contextualize this, stating that in some cases, the age limit of 18 would apply, while in others, there may be a lower threshold. It would be prudent of the government to do so, otherwise, we would be depriving an entire generation of people the access to knowledge. It is preferable to have legislation that has a significant level of federal override of state interests. It is already a focus of the parliament's attention in the case of GST, the devolution of tax revenue away from the central pole, so this is not the end of the narrative.<sup>28</sup>

What are the hits and misses from the industry perspective or a company who has a significant user base comprising of teenagers or young adults?

## **5.10 SUMMARY OF THE COUNTRIES HAVING SPECIAL DATA PROTECTION REGULATION FOR CHILDREN**

<b>SN</b>	<b>COUNTRI</b>	<b>DATA PROTECTION</b>	<b>SPECIAL</b>	<b>AGE</b>	<b>OF</b>	<b>DEFINITIO</b>
-----------	----------------	------------------------	----------------	------------	-----------	------------------

<sup>27</sup>Dr Anusuya Yadav and Gaurav Yadav, 'Data Protection in India in Reference to Personal Data Protection Bill 2019 and IT Act 2000' (2021) IARJSET 542.

<sup>28</sup>Saharsh Saxena, 'Right to Privacy and The Personal Data Protection Bill of 2019: A Critique' (2021) SSRN Electronic Journal 31.

O.	ES	REGULATION	DATA PROTECTION REGULATION FOR CHILDREN	CHILD FOR CONSENTING	OF CHILD
1.	Indonesia	NA	NA	18 years	A child is an individual who has not reached the age of 18.
2.	Japan	Act on Protection of Personal Information (APPI)	NA	20 years 18 years (1 <sup>st</sup> April 2022)	Anyone below the age of 18 years.
3.	Russia	Law on Personal Data	NA	18 years	Person below the age of 18 years.
4.	United Kingdom	Data Protection Act, 2018	Children's Code, 2020	13 years	Anyone under the age of 18.
5.	Ireland	General Data Protection Regulation, 2018	NA	16 years	A child is somebody under the age of 18.
6.	Spain	Law on Personal Data Protection of Montenegro (LPDP)	NA	14 years	A child is somebody under the age of 18.
7.	Sweden	Dataskyddsförordning,	NA	13 years	Anybody

		2018			under the age of 16.
8.	Hong Kong	The Personal Data (Privacy) Ordinance, 1996(PDPO)	NA	16 years	Below the age of 18 years.
9.	Brazil	Lei Geral de Protecao de Dados Pessoais(LGPD)	NA	14 years	Children are person below the age of 14 years.
10.	Singapore	Personal Data Protection Act, 2020(PDPA)	NA	13 years	A person less than 21 years of age.
11.	France	French Data Protection Act, 2018	NA	15 years	Child is under the age of 18 years.
12.	Taiwan	The Personal Data Protection Act(PDPA)	NA	7 years	Child is under the age of 12.
13.	India	Data Protection Act, 2018	The Personal Data Protection Bill, 2019	<b>18 years</b>	Child is under the age of 18 years.
14.	Israel	Protection of Privacy Law,1981(PPL)	NA	14 years	NA
15.	Switzerland	Federal Act on Data Protection(FADP)	NA	16 years	Child is under the age of 18 years.
16.	United	NA	Children's	13 years	Anyone

	States of America		Online Privacy Protection Act(COPPA)		under the age of 16.
17.	Argentina	Ley de Proteccion de los Datos Personales, 2000	NA	13 years	
18.	Canada	Canadian Consumer Privacy Protection Act (CPPA)	The Personal Information Protection and Electronic Documents Act (PIPEDA) still a bill.	14 years	A person under the age of 16.
19.	Italy	General Data Protection Regulation, 2018	NA	14 years	Below the age of 18 years.
20.	Mexico	Ley Federal de Proteccion de Datos Personales en Posesion de los Particulares / The Federal Law on the Protection of Personal Data held by Private Parties, 2010	NA	16 years	A child is under the age of 12.
21.	South Africa	The Protection of Personal Information Act (POPIA)	NA	16 years	A child is defined as being under the age of 18 years.
22.	Australia	The Privacy Act, 1988	NA	16 or 17 years	A person who is below

					the age of 18.
23.	Germany	The German Privacy Act / Bundesdatenschutzgesetz (BDSG)	NA	16 years	A person who is below the age of 16 or till 18 if they are full time student.
24.	New Zealand	Privacy Act, 2020	NA	16 years	A person who has not attained the age of 18.
25.	Thailand	The Personal Data Protection Act(PDPA)	NA	10 years	Person under the age of 20, if they are not married.
26.	South Korea	The Personal Information Protection Act(PIPA)	NA	14 years	Anyone who is below 18 years of age
27.	China	The Personal Information Protection Law,2021 (PIPL)	The Provisions on Cyber Protection of Personal Information of Children	14 years	A child is under the age of 14.
28.	Egypt	Personal Data Protection Law, 2020 (PDPL)	NA	18 years	A child is defined as being under the age of 18 years.

29.	Malaysia	Personal Data Protection Act, 2010	NA	18 years	Under the age of 18 years.
30.	Philippines	Data Privacy Act of 2012 / Republic Act No. 10173	NA	16 years	Under the age of 18 years.
31.	Austria	Austrian Data Protection Act (ADPA)/ Datenschutzgesetz (DSG)	NA	14 years	Persons who are 16 to 18 years of age.

## Chapter 6

### Intermediaries and present privacy policies: Are they infringing on individuals' rights to privacy?

#### **6.1 What is the definition of an intermediary?**

An intermediary is a third-party service that facilitates the delivery of a message, the negotiation of an agreement, or both<sup>1</sup>.

Consider the following scenario: a toothpaste manufacturing company delivers its products to a neighboring store, and you want to buy the toothpaste. The neighborhood store or shopkeeper has neither produced nor distributed the toothpaste (i.e., they are neither a manufacturer) (i.e., nor a consumer). They are just robbing the manufacturer of toothpaste and selling it to us. The shopkeeper functions as a middleman in this case. Intermediaries are firms that facilitate communication between the two parties. A third party facilitates the transaction between two parties. They were essential in bringing the two sides together.

In this circumstance, what function do middlemen play? The phrase "Internet Intermediaries" refers to these entities. Facebook is a social networking site where you may communicate with your friends. In this instance, Facebook acts as a middleman<sup>2</sup>. Legal safeguards exist for intermediaries.

One may get a better understanding of intermediaries by the application of case law.

#### *1. Avnish Bajaj vs. State (N.C.T.) Of Delhi<sup>3</sup>*

A fourth year IIT Kharagpur student put an offensive MMS for sale on baaze.com. @125/piece. There was no immediate indication that the video was an MMS transmission. That is, until a click is made. It was taken from Baazi.com's website after being brought to their notice. Because pornography is banned in India and the two subjects in the film were minors, the Delhi police's crime section took note and filed a charge sheet against the IIT student who released the movie

---

<sup>1</sup>Yogesh Pai and Nitesh Daryanani, 'Online Intermediary Liability and Privacy in India' (2018) SSRN Electronic Journal 73.

<sup>2</sup>Pritika Rai Advani, 'Intermediary Liability in India' (2013) Economic and Political Weekly 339.

<sup>3</sup>(2005) 3 CompLJ 364 Del

online. Additionally, a second charge sheet was filed, this time against the owner of the baaze.com account.

Under section 79 of the IT Act<sup>4</sup>, The intermediaries are excluded from liability for any data or information they transmit to third parties. Nevertheless, this safe harbour is subject to Sections 79(2) and (3) of the IT Act<sup>5</sup>.

The question now is whether blaming the website's owner is justified.

Because the website owner was unaware that the content was offensive, they erased it immediately upon discovering. Regardless, the website remains a probable suspect. Is it appropriate for authorities to imprison a small grocery store owner for selling poisonous toothpaste if the shopkeeper is uninformed of the toothpaste's flaws or the inclusion of dangerous ingredients OR should the toothpaste manufacturer carry total responsibility?

The answer is self-evident logically. The court has also ruled on this, and in the case of baaze.com, the court determined that the domain owner is also the website owner, and hence cannot be held accountable if users contribute objectionable content. It is totally up to the users<sup>6</sup>.

Conduit Laws — Pursuant to section 79 of the Information Technology Act<sup>7</sup>, all of these intermediaries are shielded by particular immunities known as the Conduit Laws since they do not control the content unless a complaint is filed in line with statutory authorities. A well-known instance in which a blog post published defamatory accusations against a local cardiologist, Dr. Ashwin. His greatest complaint was with Google Inc. for allowing those sites to post such defamatory content, to which Google responded that they were only a conduit/mediator and were unable to monitor what is continually being published.<sup>8</sup>

---

<sup>4</sup>MA Yadugiri and Geetha Bhasker, 'The Information Technology Act, 2000' (2011) English for Law 482.

<sup>5</sup>ibid.

<sup>6</sup>Yogesh Prasad Kolekar, 'Protection of Data Under Information Technology Law in India' (2015) SSRN Electronic Journal 705.

<sup>7</sup>Yadugiri and Bhasker (n 4).

<sup>8</sup>Pratik Prakash Dixit, 'From Gatekeepers to Publishers: Liability of Internet Intermediaries in India for Hosting Defamatory Content' (2021) Computer Law and Security Review 87.



## 2. *Shreya Singhal vs. UOI*

In the well-known *Shreya Singhal vs. UOI* case, the Supreme Court struck down Section 66A of the IT Act 2000, holding that the words/clauses employed in the following section lacked clarity<sup>9</sup>.

The section is principally concerned with the penalty of offences performed as a consequence of abusive, fake statements conveyed through a communication device or computer resource that cause another person to suffer irritation, danger, criminal intimidation, insult, harm, or inconvenience. The individual who committed such crimes is legally responsible under this provision of the IT Act.

In this case, the court concentrated on a vital issue regarding the qualities of real knowledge as defined by the Intermediary regulations. It was determined that knowledge exists when a court or appropriate government notifies an intermediary that such content is unlawful, and that if the intermediary fails to remove such content after receiving actual knowledge that it is unlawful, the intermediary's status will be terminated, and the intermediary's due diligence will be violated.

## 6.2 What justifies regulation?

With the increased usage of social media platforms and the movement of a huge industry to IT-based platforms, social media giants and technology corporations have expanded their footprints in India, and with this increased public use comes the potential for abuse of these technologies. Child pornography, regularly, false news, revenge porn, harsh language, libellous, and obscene content have harmed women's dignity and religious feelings, leading to the emergence of dissension and anti-national elements.<sup>10</sup> It is a challenge for law enforcement organizations to put an end to all of these operations. There was no such specialized system in India for addressing customer complaints within a specified timeframe. Due to a lack of transparency and the absence of a robust grievance mechanism, users have been fully dependent on the whims and fancies of these social media platforms, with no recourse. As a consequence, new legislation will serve as a disincentive to such material while also improving the process's equity and transparency.

---

<sup>9</sup>Debarati Halder, A Retrospective Analysis of Section 66 a: Could Section 66 a of the Information Technology Act Be Reconsidered for Regulating Bad Talk in the Internet? (2018) SSRN Electronic Journal 323.

<sup>10</sup>Amruta Das and Rubi Talukdar, 'The Sedition Laws in India with Special Reference to *Shreya Singhal vs. Union of India*' (2019) International Journal of Psychosocial Rehabilitation 56.

### 6.3 Governing history

MeitY (Ministry of Electronics and Information Technology) solicited public feedback on the Draft Information Technology (Intermediary Guideline) Rules, 2018<sup>11</sup> in December 2018. Additionally, they evaluated and compared it to the 2011 Information Technology Trends report (Intermediary Rules)<sup>12</sup>. MeitY and MIB, on the other hand, had no discussions prior to issuing the IT Rules, 2021. They breached the Ministry of Law and Justice's 2014 pre-legislative consultation guidelines by evading scrutiny from multiple parties by missing the required 30-day limit on this contentious subject.

In April 2018, the MIB appointed a ten-member board to formulate and recommend a regulatory framework for online media/news portals, including digital broadcasting, entertainment/information websites, and news/media aggregators, but the board was later dissolved, and the responsibility was transferred to MeitY. MeitY and MIB pioneered this division of legal authority between OTT services and social media platforms. In 2020, the Government of India (Allocation of Business) Rules, 1961 were amended to provide the MIB regulatory authority over OTT platforms and online news media.

According to the Government's official press release on the IT Act, 2021, in April 2018, the MIB appointed a ten-member board to formulate and recommend a regulatory framework for online media/news portals, including digital broadcasting, entertainment/information websites, and news/media aggregators, but the board was later dissolved and the responsibility was transferred to MeitY.

The Indian Express reported on December 24, 2018, on a secret meeting during which suggested revisions to the regulations under Section 79 of the Information Technology Act, 2000 (IT Act)<sup>13</sup> were discussed. Section 79 of the IT Act creates a safe harbor for intermediaries that host user-generated content, exempting them from liability for the actions of users on their platform so long as they adhere to government-mandated requirements.

---

<sup>11</sup>Rishab Bailey, Smriti Parsheera and Faiza Rahman, 'Comments on the (Draft) Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018' (2019) SSRN Electronic Journal 65.

<sup>12</sup>Devdeep Ghosh, 'The Information Technology (Intermediaries Guidelines) Rules, 2011: A Disaster on All Fronts' (2013) SSRN Electronic Journal 336.

<sup>13</sup>Yadugiri and Bhasker (n 4).

While the Ministry of Electronics and Information Technology (MeitY) first denied knowledge of the conversation and proposed changes, it eventually acknowledged them and sponsored a public poll.

#### **6.4 Aspects of the Information Technology Rules of 2021 from a Legal Perspective**

MeitY promulgated the Information Technology Rules, 2021 in exercise of the powers given on it by Section 87 of the Information Technology Act, 2000<sup>14</sup>. However, several lawsuits have been filed contesting the legitimacy of these regulations, which are believed to be unclear and to include an excessive delegation of authority, which may ultimately result in non-judicial entities exercising judicial tasks.

Consultation was insufficient

MeitY then issued a public consultation on suggested revisions to the liability exemptions for internet platforms and service providers. Any service provider that transmits, hosts, and publishes user material without exerting editorial control over it in the same manner that conventional publishers do. This might be the Internet service provider, email provider, social networking platform, or any other web-based application that enables a person to publish or to share.

#### **6.5 The Current State of Affairs**

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the "Intermediary Rules") explains the substance, the protections they attempt to build, and how they affect the internet user experience and basic rights in India.

##### **6.5.1 What Are the Intermediaries' Rules?**

The Intermediary Rules superseded the 2011 Information Technology (Intermediary Guidelines and Code of Ethics for Digital Media) Rules (or the 2011 Rules). I have offered a much more detailed and legal examination of the Intermediary Rules in this Chapter.

##### **6.5.2 What is the framework of the Intermediary Rules?**

---

<sup>14</sup>Yadugiri and Bhasker (n 4).

While Part I of the Intermediary Rules is largely concerned with the definition of terminology, Parts II and III include real compliances and obligations. Part II governs intermediaries, particularly those in the social media space. Messaging networks like WhatsApp, Signal, and Telegram, as well as media platforms like Facebook, Instagram, and Twitter, serve as intermediaries in social media. Part III regulates digital news organisations and over-the-top (OTT) services such as Netflix, Amazon Prime, and Disney+Hotstar. It is unclear to which news companies these Rules apply.

In the social media and communications sphere, intermediaries

1. Creation of new classes: New classes, such as social media intermediary [Rule 2(w)] and major social media intermediary [Rule 2(v)], have been created. On February 26, 2021, it was declared that a social media intermediary must have five million registered users in order to be categorised and regulated as a large social media intermediary.<sup>15</sup>

2. Requirement for a nanny: Do you dislike email spam? Do you detest ever more unintelligible Terms of Service and Privacy Policies? Prepare to receive them more often than once a year, since the new regulations compel each intermediary to inform you at least once a year [Rule 3(c)]. This implies that almost every online service will send you occasional emails telling you not to engage in illegal behavior or your account will be terminated.

3. Grievance redressal mechanism: While the 2011 version (Rule 11)<sup>16</sup> requires an intermediary to establish a grievance redressal person, there are now a plethora of extra compliance requirements. Previously, the Grievance Officer was responsible for receiving and addressing complaints from users against the Rules; today, the Grievance Officer is responsible for noting complaints within 24 hours and resolving them within a month.

4. Significant Social Media Intermediaries must have an in-house grievance resolution team: Along with the requirements placed on intermediaries, large “social media intermediaries” are obliged to select three officers with unique roles [Rule 4(1)]<sup>17</sup>. The officers are as follows:

---

<sup>15</sup>Divij Joshi, ‘Towards a Safer Social Media – Submissions to the Ministry of Information and Technology, Government of India, on the Draft Information Technology Intermediary Guidelines (Amendment) Rules, 2018’ (2019) SSRN Electronic Journal 78.

<sup>16</sup>Rishabh Dara, ‘Intermediary Liability in India: Chilling Effects on Free Expression on the Internet’ (2012) SSRN Electronic Journal 434.

<sup>17</sup>Joshi (n 15).

- A Chief Compliance Officer who is liable for ensuring compliance with the Information Technology Act, 2000<sup>18</sup> (the IT Act) and its standards and for any ensuing actions.
- a single point of contact for 24-hour collaboration with law enforcement officials; and
- a Resident Grievance Officer, with similar responsibilities to the Grievance Officer for intermediaries described above; additionally, a Resident Grievance Officer of a significant social media intermediary is required to notify a user prior to removing their content, provide them with an opportunity to dispute such action, and provide the complainant with the reasons for the decision made in response to their complaint [Rules 4(6) and 4(8)]<sup>19</sup>.

Important: Three officials from social media intermediaries are now legally obliged to live in India, and significant social media intermediaries are now needed to have a physical contact address in India “[Rule 4(5)]<sup>20</sup>. The officers' contact information and physical address must be clearly disclosed on the intermediary's website or mobile Internet application.

5. Contracted timelines for assisting law enforcement agencies: Whereas the 2011 Rules<sup>21</sup> required intermediaries to act within 36 hours and, where applicable, work with the user or owner of such information to remove it, the new Intermediaries Rules require intermediaries to \*complete\* the takedown process required by Section 79(3) of the IT Act within 36 hours<sup>22</sup>.

In addition, a new takedown obligation has been established, requiring the intermediary to erase material including nudity, portrayals of sexual conduct, or impersonation within 24 hours of receiving a request from the applicable user. [Rule 3(2)(b)].

6. Greetings, older sibling! The obligatory data retention duration has been increased to 180 days (six months!) for investigation reasons [Rule 3(1)(h)]. This obligation remains even if a user deletes their account; this requirement is crucial to consider given India's lack of a data privacy legislation and control over how surveillance is conducted.

---

<sup>18</sup>Yadugiri and Bhasker (n 4).

<sup>19</sup>Advani (n 2).

<sup>20</sup>Dixit (n 8).

<sup>21</sup>‘The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011’ (2011) 3.

<sup>22</sup>Chakshu Roy and Harsimran Kalra, ‘Rules & Regulations Review’ <[http://www.prindia.org/uploads/media/IT\\_Rules/IT\\_Rules\\_and\\_Regulations\\_Brief\\_2011.pdf](http://www.prindia.org/uploads/media/IT_Rules/IT_Rules_and_Regulations_Brief_2011.pdf)>. Accessed on 2 November 2020.

7. Significant social media intermediaries must also let users to voluntarily verify their accounts by any suitable means, including the user's valid Indian cell number, and must display a visible, provable symbol showing such verification [Rule 4 (7)]<sup>23</sup>. This might result in a predicament comparable to the one encountered by humans.

This would have major consequences for anonymity and privacy (imagine being required to connect your Aadhaar to your social media accounts in order for government authorities to reply to you!), all of which are crucial for users of social media intermediates, such as political dissidents. Additionally, and possibly more concerning, without a data privacy legislation, social media firms would be able to acquire data from our government-issued identification cards without being regulated by a data protection authority.

8. End-to-end encryption: According to Section 69A of the IT Act, significant social media intermediaries should provide tracking of the source of material on their platform when requested by a court or competent body [Rule 4(2)]<sup>24</sup>. While the Intermediaries Rules indicate that a court or competent authority may issue a traceability order only for significant offences, some categories are open-ended. For instance, the public order defense has a quite wide scope.

Additionally, the Intermediaries Rules clarify that a significant social media intermediary is not required to disclose the contents of any electronic message, any other information about the message's originator, or any other information about its other users; however, the Information Technology Decryption Rules include authority to make demands for message content. When combined, the government can decrypt any sort of end-to-end encryption in order to collect information.

9. Artificial intelligence-assisted censorship: Significant social media intermediaries must now develop and implement technology-based measures, such as automated tools or other techniques, to proactively identify material depicting rape, child sexual abuse, or conduct that is sexually abusive toward children [Rule 4(4)]<sup>25</sup>.

---

<sup>23</sup>Bailey, Parsheera and Rahman (n 13).

<sup>24</sup>Narayan and Kulkarni (n 18).

<sup>25</sup>G Aswathy Prakash, Asha Sundaram and B Sreeya, 'Online Exploitation of Children and the Role of Intermediaries: An Indian Legislative and Policy Perspective' (2021) *International Review of Law, Computers and Technology* 78.

10. Penalties: The 2011 Rules<sup>26</sup> made no mention of penalties for intermediaries who violated the Rules' restrictions; the resulting consequence was rather straightforward: they lost immunity! The Intermediaries Rules, 2021<sup>27</sup> specifically say that immunity would be revoked and specify the severity of the repercussions, which may include criminal prosecution under the Information Technology Act and the Indian Penal Code [Rule 7].

## **6.6 Digital News and Video Streaming Platforms**

Possibly the most important change to the Rules is the regulation of OTT platforms and digital news media whether they utilize intermediate websites/apps such as Twitter or Facebook or when they host news media material on their own website/app. It's worth noting that the 2011 Rules included no mention of digital news media or over-the-top (OTT) services.

1. The Rules were prepared in accordance with the Information Technology Act, 2000, and as such, MeitY is the nodal ministry for their administration; however, according to the Intermediary Rules, the Ministry of Information and Broadcasting will be responsible for Part III [Rule 8(1)].
2. The IT Act's regulatory authority has been expanded: Previously, digital news media and over-the-top (OTT) platforms were not governed under the requirements of the IT Act. This was updated as a result of a notice under the Allocation Rules for Business. However, this announcement just specifies which ministry would govern the sector; it does not provide the power to do so. This requires a straightforward legislative enactment.
3. Excessive delegation of authority: The Rules established a non-judicial adjudicatory process for resolving grievances regarding content published by Digital News Media and OTTs, as well as an adjudicatory body dubbed the oversight committee, despite the fact that the IT Act does not expressly authorize the Government to do so.

Apart from that, the section's highlights have been summarized below.

---

<sup>26</sup>Rebecca Wong, 'Data Protection: The Future of Privacy' (2011) Computer Law and Security Review 321.

<sup>27</sup>Krishnan (n 15)."

1. A wide range of applications. Not just big digital news organizations: No user or readership criterion has been proposed to separate digital news sources by size and scale, as was done in Part II for social media intermediaries and important social media intermediaries. All publishers of news and current affairs material are covered by the Intermediaries Rules, as long as they have a physical presence in India.
2. Regulation of foreign news media: While geographical presence is a required prerequisite for digital news media to be controlled under the Intermediaries Rules, it is not a mandatory criterion [Rule 8(2)]. The Intermediaries Rules apply to a digital news media organization that makes its material accessible in India in a systematic and consistent way.
3. Code of Ethics: Digital News Media and Over-the-Top (OTT) providers are expected to adhere to a Code of Ethics, which is specified in the Rules' Appendix. The requirements in the Code of Ethics are vague and too broad, and they will inhibit publishers' freedom of expression and consumers' access to information.

As regards digital news media, they must also comply to the Press Council of India's Norms of Journalistic Conduct and the Program Code and abstain from publishing or transmitting anything that is prohibited by law. This is crucial for OTTs since they are now forced to categorize material as 'U', 'U/A 7+', 'U/A 13+', 'U/A 16+', or 'A' (Paragraph II(B) of Appendix). Additionally, they must guarantee that material categorized as U/A13+ or above has access control measures and that content classified as A (limited to adults) includes an effective age verification system.

4. Grievance Redress Procedure: The Intermediary Rules provide a three-tier grievance resolution mechanism to guarantee conformity with the Code of Ethics. During the Rules announcement news conference on February 25, 2021, the Union Minister of Information and Broadcasting hailed the three-tier approach as self-regulation by publishers with minimum government intrusion. Closer study indicates, however, that the Rules foresee much more than minimal government intrusion.<sup>28</sup>

Similar to the need for intermediaries under Rule 3, digital news organizations and OTT platforms must develop a grievance redressal process and select an Indian-resident Claim Officer who is responsible for resolving each grievance received within 15 days. If the complaint does

---

<sup>28</sup>Krishnan (n 15).



not obtain a suitable answer within 15 days, he or she may appeal to Level II, which is the self-regulatory body (Rules 10 and 11)<sup>29</sup>

At the second level, the self-regulatory body must be an independent organisation comprised of publishers or their associations and led by a retired Supreme Court or High Court judge or an independent eminent individual from the media, broadcasting, entertainment, child rights, human rights, or other pertinent fields. This organisation must be registered with the MI&B, and the MI&B will ensure that the self-regulatory body was properly created (Rule 12)<sup>30</sup>

5. Third Tier: Level III is the self-regulation system for digital news organizations and OTT platforms. The supervision mechanism is an Inter-Departmental Committee made up of delegates from the Ministries of Information and Broadcasting, Women and Child Development, Law and Justice, Home Affairs, Electronics and Information Technology, External Affairs, and Defense<sup>31</sup>.

While publishers are required to self-regulate at the first layer, the Rules' provisions make self-regulation impractical: anybody may submit a complaint with the publisher, and the publisher must answer within 15 days or risk censure. This implies that the typical internet user will have their news coverage edited to accommodate for the Rules' arbitrary character.

6. Excessive government regulation of digital news and over-the-top (OTT) content: While level II of the three-tier mechanism is presented as the second layer of self-regulation, it is actually the first layer of government control; the proposed chairman of the self-regulatory body is a retired High Court or Supreme Court judge, and while the body is ostensibly expected to be appointed/elected by the media community, the Ministry for Information and Broadcasting retains appointment authority.

7. Executive use of judicial powers: The supervisory system is led by the Joint Secretary, Ministry of Information and Broadcasting, who is in turn monitored by the Secretary.

8. Emergency blocking powers: The MI&B has emergency blocking powers under the Intermediary Rules in cases when no delay is acceptable. If the Secretary considers that it is

---

<sup>29</sup>Ravi Shankar and Tabrez Ahmad, 'Information Technology Laws: Mapping the Evolution and Impact of Social Media Regulation in India' (2021) DESIDOC Journal of Library and Information Technology 607.

<sup>30</sup>Ashwini (n 16).

<sup>31</sup>Ministry OF Women, 'Government of India Ministry of Women and Child Development' [2013] Rapid Survey on Children (RSOC) 2013-14 National Report.

necessary or expedient and reasonable, she/he may issue orders prohibiting people, publications, or intermediaries in charge of hosting such material from receiving online content without giving them a chance to be heard (Rule 16)<sup>32</sup>.

9. Scope of punitive measures: The tier-II self-regulatory body and the level-III Inter-Departmental Committee have been empowered with broad punitive powers over digital news media and OTT platforms, including the authority to warn/censure/admonish/reprimand the publisher, require a warning card or disclaimer, require an apology, reclassify ratings, or even censor content, as they see fit, and recommend action under Section 69A of the IT.

10. Government registration: Union Minister Prakash Javadekar revealed at a press conference that the government was ignorant of the identity of digital news organizations and over-the-top (OTT) platforms. To close this information gap, the Intermediary Rules compel digital news organisations and over-the-top (OTT) platforms to register with the MI&B and give information about their entity and intermediary accounts (Rules 5 and 18).

### **6.7 Intermediary in social media has been affected**

While the phrase exercise reasonable caution and discretion has been interpreted as creating ambiguity when the publisher's responsibility is at stake, publishers of curated online content are required to exercise reasonable caution and discretion when the content in question relates to the activities, practices, beliefs, or views of any racial or religious group.

On February 26, 2021, the government declared that a social media intermediary must have a minimum of 50 lakh (5 million) registered users in order to be classified and regulated as a significant social media intermediary.<sup>33</sup> These categories allow the government great leeway in selecting which establishments must follow particular regulations. This power is reinforced by Rule 6, which specifies that the government may compel any intermediary to comply with the responsibilities placed on a significant social media intermediary. To satisfy the condition, there must be a substantial material threat of harm, a hazy word that permits the government to enact discriminatory compliance legislation.

---

<sup>32</sup>M Mohan and K Someshwer Rao, 'A Study on Operational Performance of Selected Public and Private Sector Banks in India' (2021) *International Journal of Interdisciplinary and Multidisciplinary Research* 55.

<sup>33</sup>Joshi (n 27).

In addition, Rule 3(1)(h) mandates that intermediaries save data for 180 days (six months!) after a user's account has been cancelled for investigative purposes<sup>34</sup>. In the lack of a data privacy legislation and any oversight of how surveillance is performed in India, it is vital to recognize this obligation and comprehend its implications.

## **6.8 OTT platform**

The new OTT content guidelines divide material into four categories: 'U', 'U/A 7+', 'U/A 13+', 'U/A 16+', and 'A' (Appendix II, Paragraph II(B)). OTT providers are expected to install access control measures for material rated U/A13+ or above and a credible age verification system for content rated A (restricted to adults) in order to prevent minors from accessing such content<sup>35</sup>.

Because the newer OTT video streaming platforms do not have the underlying legislation that the Cable Television Network Act of 1995<sup>36</sup> and the Cinematograph Act of 1952 do, there are no safeguards in place to prevent the executive branch from expanding the scope of the rules and censoring content it deems objectionable.

Parental restrictions over particular material will be necessary, as will the presentation of the program's rating. The bill contains a clause forcing important intermediaries to give a voluntary verification option for their users, a move that might jeopardize their privacy and anonymity. This would include consumers revealing their phone numbers or submitting corporation's images of government-issued identity. This clause may pave the way for the profiling and targeting of users via the use of sensitive personal data. Additionally, this clause increases the possibility of data breaches and places us at the whims of the major social media and message software companies.

## **6.9 Current-events and news-related content**

---

<sup>34</sup>Naganna Chetty and Sreejith Alathur, 'Policies to Mitigate Select Consequence of Social Media: Insights from India', *Advances in Intelligent Systems and Computing* (2020).

<sup>35</sup>Meera Mathew, 'Freedom of Information, Right to Express and Social Media in India' (2020) *Interactive Entertainment Law Review* 47.

<sup>36</sup>Snehil Kunwar Singh and Harpreet Singh Gupta, 'Telecast Bans of Television News in India: Issues and Reform' (2021) *Indian Law Review* 534.

According to The Wire, which challenged the legality of the IT Rules 2021 in a writ petition, news and digital media businesses are not protected by the Information Technology Act of 2000. According to the online news platforms, these Rules are only a smokescreen for the Ministry's indirect effort to govern and regulate these content providers.

The Rules include a hazy definition of publisher of news and current affairs content that appears to exclude digital copies of newspapers; this distinction appears to be unfair to smaller news organizations that rely entirely on internet revenue; and this hazy definition gives the Government sufficient leeway to be ambiguous through the exercise of discretionary power granted by these Rules. Certain unexpected rules-imposed registration requirements on news and current affairs content producers regardless of their size, as well as content removal restrictions on online news websites, online news aggregators, and curated audio-visual platforms. Part III of these rules grants the concerned Authority the authority to order the removal of any news and current affairs content published online by these news and current affairs content providers (who are not considered intermediaries) and contains no meaningful explicit checks and balances against executive overreach.

#### **6.10 How social media companies sought to skirt the rules**

Following the central government's publication of IT recommendations, Twitter and Facebook attempted to circumvent the requirements to the greatest extent feasible, with Twitter failing to comply months after the guidelines were published. Twitter Inc. was entangled in a court struggle with the Indian government over the new information technology legislation, in which the company was found to have violated compliance requirements. Due to Twitter's violation of the laws, the Indian government sent a bombardment of letters to the digital giant, which, as is customary, sought further time to comply. In addition to Twitter India's noncompliance, the Uttar Pradesh government has initiated action against the company<sup>37</sup> for failing to remove tweets spreading disinformation regarding the state crime.

*Twitter lacked a grievance officer at the time.*

---

<sup>37</sup>Sanjeev Ratna Singh, 'Bjp vs Opposition Parties on Twitter: A Comparison of Social Media Strategies for Political Mobilisation during 2017 Uttar Pradesh and Gujarat Assembly Elections' (2019) International Journal of Advanced Science and Technology311.

Following that, the Court chastised Twitter in July 2021 for violating the standards and lying-in court. When informed that the social media giant lacked a full-time resident grievance officer as required by the new IT Rule in effect at the time, the Delhi High Court chastised the microblogging platform for failing to appoint a grievance officer from June 21, when the existing officer was removed, to July 6<sup>38</sup>.

Twitter was not able to create a nodal officer in compliance with the IT requirements until August 6th. At the time, Facebook sought to circumvent the requirements by declaring that they intend to comply with the standards but need more interaction with the government. We intend to adhere to the terms of the IT [Information Technology] guidelines and to continue discussing a few of the topics that need greater interaction with the government,” a Facebook<sup>39</sup> representative added. Finally, they claimed to have for failing to delete tweets disseminating false information about a state offence.

At the time, Twitter lacked a grievance officer.

In July 2021, the Court reprimanded Twitter for breaking the norms and lying-in court. When told that the social media behemoth lacked a permanent resident grievance officer, they met the requirements by appointing a grievance officer; nevertheless, we will now look at how they are skillfully misleading the authorities.

### **My encounter with Facebook's grievance resolution process" and how the internet giant dupes the authorities.**

I then sought for the Grievance Official's email address, since the Guidelines stipulate that the officer must be an Indian citizen with a physical office address, hinting that human participation is required in addressing concerns<sup>40</sup>.

---

<sup>38</sup>ibid.

<sup>39</sup>Sanjay Sharma, 'Facebook: A Perennial Abuser of Data Privacy', *Data Privacy and GDPR Handbook* (2019).

<sup>40</sup>Simon Kemp, 'The State of Digital in April 2019: All the Numbers You Need to Know' (*We are social*, 2019).

## How do I contact the Grievance Officer and Facebook in India?

Computer help ▾

Copy link

The quickest way to address your concern is by visiting the Help Centre or by using the [report links found throughout the site](#). Dedicated teams work to handle the reports made to Facebook using our online tools.

The role of the Grievance Officer under the Information Technology Act, 2000, as applicable in India, is to redress grievances of users or victims in India and not to receive legal process.

If you choose to contact the Grievance Officer with complaints or concerns, including those regarding violations of Facebook's [Terms of Service](#), Facebook's [Community Standards](#) or questions about accounts, please do so via [this form](#), signed with an electronic signature.

Below is the contact information for Facebook's Grievance Officer, published in accordance with the requirement under Indian law. Please note that this email is only used for the purpose of addressing questions about the grievance redressal mechanism process.

Spoorthi Priya

FBGOIndia@fb.com

Additionally, you can also contact Facebook in India via post at:

216 Okhla Industrial Estate, Phase III

New Delhi – 110020

Was this helpful?

*Figure 6.1* Email to grievance officer

I sent an email to the mentioned address – FBGOIndia@fb.com. Interestingly, when I sent a detailed email outlining my grievance, I received another entirely automated response.

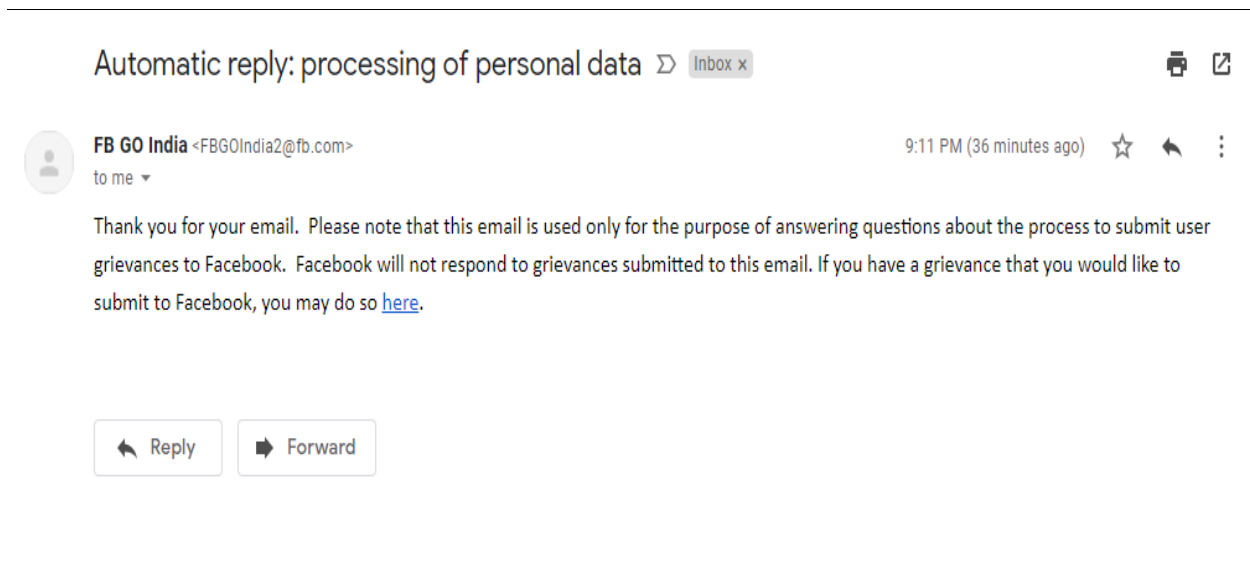


Figure 6.2 Automated reply

When I clicked on the link provided in the automated response” to my lengthy email to the grievance officer, I was directed to a form that I completed.

The image shows a web form titled "Indian Grievance Officer Complaint". The form has a blue header with a back arrow and the title. Below the header, it says "Use this form to submit a complaint to the India Grievance Officer." The main section is titled "What issue do you wish to report?" and contains a list of radio button options in both English and Hindi. The options are: "मेरा अकाउंट हैक कर लिया गया है", "I've lost access to a page or a group I used to manage", "I've found a fake profile or a profile that's pretending to be me", "मुझे धमकाया जा रहा है या मेरा उत्पीड़न किया जा रहा है", "मुझे अनुपयुक्त या अनुचित सामग्री मिली है", "I want to report content showing me in nudity/partial nudity or in a sexual act", "मैं (या कोई अन्य व्यक्ति जिसकी कानूनी जिम्मेदारी मुझपर है) उस सामग्री में प्रदर्शित हूँ, जिसमें मैं प्रदर्शित नहीं होना चाहता", "I want to access or download my personal data", "I am a Law Enforcement official seeking to access user data", "I am a government official or a court officer seeking to submit an order, notice or direction", "I have an issue with how Facebook is processing my data", "I want to report an Intellectual Property infringement", and "I want to report another issue". At the bottom of the form, there is a blue button labeled "सबमिट करें".

Figure 6.3 Automated complaint form

Following that, I was routed to the in-app appeal, which is intended to lead me to the grievance officer. Interestingly, the in-app appeal to the Grievance Officer lacked the option I required: there was no way to determine whether or not my data was being transmitted to other counties.

In response, I received another automated answer including links to the community rules.

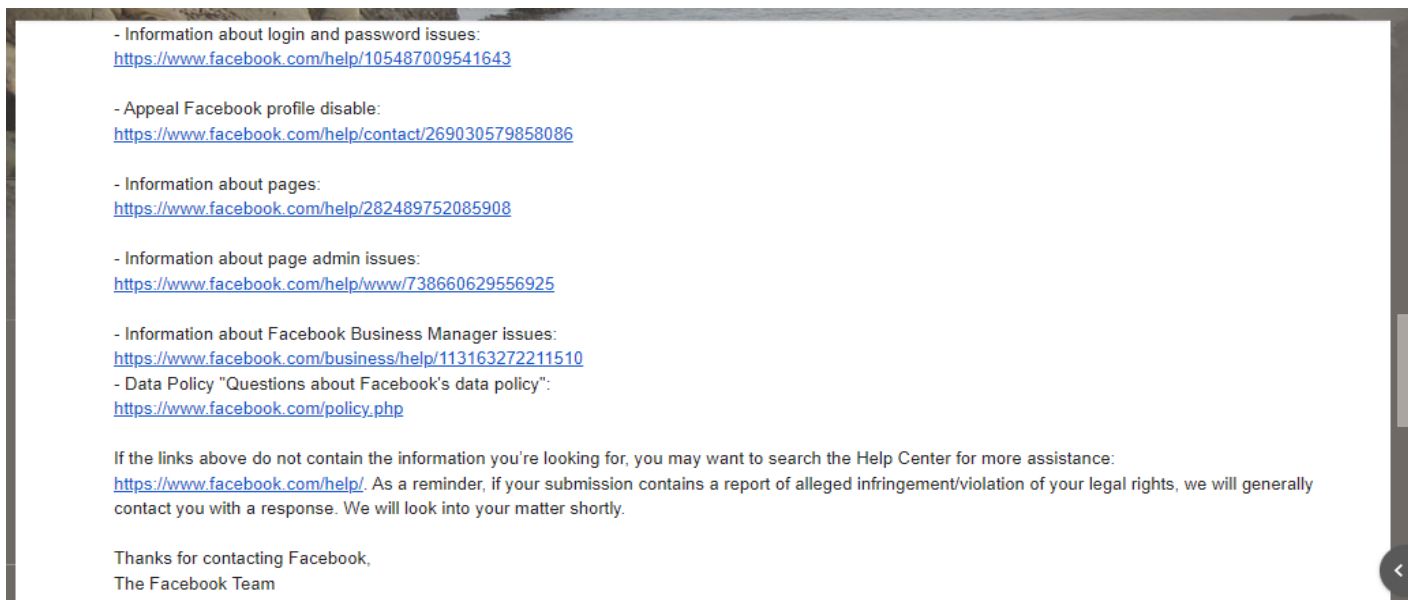
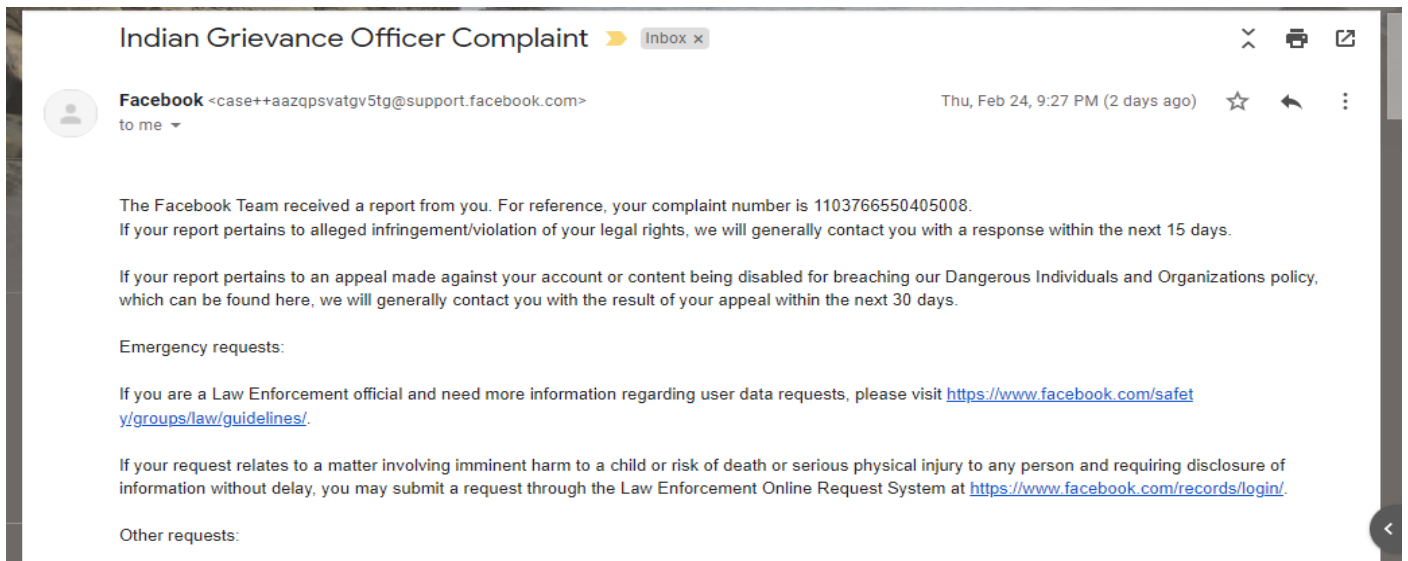


Figure 6.4 Automated response



It's worth noting that while Facebook is required by Indian law to have a Grievance Officer who resolves complaints, in practice, it's clear that they are skirting the law: there is no human intervention in resolving grievances, and when users raise a complaint, they are met with an automated response.

I personally visited Facebook's Grievance office at the address mentioned on their official site. There I could not find the Facebook office what I found the details are mentioned here below:



Just a box where

*Figure 6.5 Facebook grievance office*

The office address belonged to Amarchand, which is a law firm.



*Figure 6.6 Amarchand Office*

Since I could not find anyone from Facebook, neither any email address, nor any contact number, therefore I decided to write an email to Amarchand for which I did not receive any reply.



SUMEDHA GANJOO



To: shardul.shroff@AMSShardul.com; rohan.arora@AMSShardul. Mon 6/20/2022 12:13 PM

Cc: Garima Tiwari

Dear Sir/Ma'am,

This is to bring to your kind notice that I visited the Facebook grievance office at 216 Okhla Industrial Estate, Phase III New Delhi - 110020 on 7th June 2022. The address is of law firm Shardul **Amarchand** Mangaldas's Delhi office. There I found a box and was told to submit my grievance in that box. When I enquired about the grievance officer i.e Ms. Spoorthi Priya, I was told she sits in a different office. I asked for the office address where she sits or her contact number but I was refused. I even asked for the employee list of people working in facebook grievance redressal, but I was told that it is confidential information.

The purpose of my visit was for my Ph.D. Research to understand the efficiency of the Facebook Grievance Cell. However, as was observed, the requisite rules as mentioned in the IT Rules, 2021 have not been followed by Facebook and Amarchand. As per the IT Rules, 2021, which came into effect last year, social media companies like Facebook are mandated to appoint India-based resident grievance officers as part of their due diligence as 'intermediaries' who enjoy legal immunity from third-party content on their platform. These officers are responsible for overseeing the grievance redressal mechanism of complaints from the people who use their services. These rules were laid down so that there should be a physical contact address in India for communication (for SSMI), to make sure that users can meaningfully reach out to SSIMs to voice their concerns, as many SSIMs are international organizations. As mentioned in Rule 4(1) of the IT Rules, 2021, the Chief Compliance Officer and the nodal contact person cannot be the same person. In contrast, the same person may perform the roles of the nodal contact person and the Resident Grievance Officer. However, keeping in view the functional requirements of the nodal contact person and the Resident Grievance Officer, it is desirable that SSMI appoints separate persons for the two roles. The

Government, through this rule, expects the intermediary to provide separate contact details for grievances submitted by users and the requests/orders made by the Government or authorized Government agencies since the nature of requests might vary in view of different compliance timelines.

We would like to enquire about the extent to which these rules have been followed by you and Facebook as we could not meet Ms. Priya Spoorthi. Kindly share further details about her, particularly whether she is an employee of Facebook or Amarchand? Also, is Amarchand handling the Grievance cell of Facebook, if yes then to what extent? We also request you to provide the list of employees working in the Facebook grievance department or they are also the employees of Amarchand only? In this regard, would Facebook and Amarchand become one entity in India?

Looking forward to a positive reply from your end so that my research is benefitted.

*Figure 6.7 Mail to Amarchand*

Twitter deleted the popular political parody account Eminent Intellectual in September 2021.”<sup>41</sup>.An audio recording published by the account Eminent Intellectual has the parody declaring, "Namaste, everyone, this is Princess Awake Liberal" (completely woke). If you are reading this, you are no longer following me on Twitter. Unfortunately, I was suspended without prior notice or communication. I've made an appeal, but as we all know, "that's like appealing with the Taliban for a casual Friday. Not going to occur!"<sup>42</sup>

She highlighted, I tweeted about Rana Ayyub's years of Elle magazine marketing, emphasizing that her brother Arif Ayyub is the magazine's publisher." It is important to note that the tweet was not published. But was precisely heard. It was readily apparent to me and I uninstalled it an hour after discovering what was occurring.

As far as I am aware, Rana Ayyub attacked the Totalwoke account in the past. I was well aware that I had committed Twitter blasphemy and that my account deserved to be banned (only one punishment) ...You are aware of what this signifies! Anyway, Totalwoke and I are now working out how to communicate with our pals here. You'll hear from me in a few days, and I'm certain we'll have your information.

Another illustration

Neha Shree is a Bhojpuri and Rajasthani actress who has acted in many television series. In November 2021, she filed a lawsuit in the Delhi High Court, citing the Delhi government and Facebook as defendants and requesting that the court restore her Facebook profile and access to it. According to allegations, the hacker was sending filthy texts and photographs via her account. According to Neha Shree, she also reported the incident to the Cyber Cell of the Delhi Police but was informed that no action would be done. According to the appeal, her reputation has been severely damaged by his Facebook page and inflammatory post. A FIR was also lodged, but no action was taken.<sup>43</sup>

Neha stated in her petition that after receiving no response to her complaint, she went to the Facebook office address in Delhi listed on their page; however, there was no one there and no

---

<sup>41</sup>Dr Govind Singh Rajpurohit and Dr Raj Kumar Yadav, ‘A Socio-Legal Analysis of WhatsApp Privacy Policy 2021 in India: A Contemporary Study’ (2021) SSRN Electronic Journal 334.

<sup>42</sup>ibid.

<sup>43</sup>Cayce Myers, ‘Digital Immortality vs. “The Right to Be Forgotten”’: A Comparison of U.S. and E.U. Laws Concerning Social Media Privacy’ (2016) 16 Romanian Journal of Communication and Public Relations 47.

office was located; the guard instructed her to drop her complaint in the drop box; she received a response stating that action would be taken within 30 days, but no one from Facebook took any action; and she received a second response stating that action would be taken within 30 days, but no one from Facebook took any action.

According to IT principles, intermediaries become publishers when they unilaterally select what material is accepted or prohibited on their platform. The whole sequence of events indicates that YouTube is not following to IT norms and is instead behaving as a publisher<sup>44</sup>.

### **6.11 What are the concerns, and what can be done by the government?**

While social media companies assert that they followed central government rules, case studies reveal that they sought to disrupt the process in practice. While the legislation demands human involvement and the designation of a grievance officer, social media companies have merely included the officer's name and email address. In essence, large IT companies deceive the government into assuming that regulations are being obeyed. Due to the inherent bias of the mainstream media, the government must engage with users of these social media platforms who may inform the government about the issues at hand and how the suggestions are not being implemented. The conclusion makes no mention of government intervention if grievance authorities are unable to resolve the issue, and the government should intervene quickly if this is the case.

### **6.12 Global Perspective**

With the advent of the Internet, it became evident that virtual world regulation was essential. Numerous countries recognized this, adopting a range of measures for forcing internet platforms and intermediaries to adhere to a tight or flexible framework.

#### *6.12.1 Singapore*

---

<sup>44</sup>Anna Kobernjuk and Agnes Kasper, 'Normativity in the EU's Approach towards Disinformation' (2021) *TalTech Journal of European Studies* 84.

The regulation governing the content of OTT platforms is simple and direct. Singapore's media regulatory authority enacted an ethical code in 2018<sup>45</sup> mandating OTT and video streaming service providers to segregate their material similarly to theatrically released films, setting a rigorous audience watching label that must be adhered to. Additionally, this code mandates that content providers indicate the film's classification and any explicit themes, such as violence.

Singapore has adopted the Protection from Online Falsehoods and Manipulation Act (POFMA) to address and alleviate rising concerns about the spread of disinformation through social media platforms. This regulation attempts to eliminate user-generated false news information from social media platforms and to limit end-user access to the corresponding statement.

### 6.12.2 Germany

Germany approved the allied Network Enforcement Act (Netzwerkdurchsetzungsgesetz - NetzDG) in 2017<sup>46</sup> in response to the absence of self-regulation by social media companies. The Act tries to solve this by regulating online platforms behavior and forbidding the distribution of offensive and aggressive material as defined in Sec. 1 (3) NetzDG. Online platforms who fail to erase illicit information face fines of up to €50 million<sup>47</sup>. A review mechanism that allows users to object to the deletion of a post or the preservation of an illegal one, requiring social media sites to include a route for counter-presentation.

Increased user-friendliness of reporting channels that are simple to use and easily distinguishable from content; enforcement of orders against social media platforms for permissible data disclosure, such as the offender's identity; and enforcement of orders against social media platforms for permissible data disclosure, such as the offender's identity.

Increased requirements for submitting the aforementioned transparency reports, including adjustments to previous reports and increased access to anonymized data by independent research institutions to ascertain which groups are commonly targeted with illicit content.

---

<sup>45</sup>Singapore Association of Pharmaceutical Industries, 'Code of Conduct 2018' (*Singapore Association of Pharmaceutical Industries*, 2018).

<sup>46</sup>Ben Wagner and others, 'Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act', *FAT\* 2020 - Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (2020).

<sup>47</sup>Thomas Kasakowskij and others, 'Network Enforcement as Denunciation Endorsement? A Critical Study on Legal Enforcement in Social Media' (2020) *Telematics and Informatics* 47.

This draft was adopted as a scheme to amend the Audiovisual Media Services Directive<sup>48</sup>, which anticipates compliance obligations to protect against illegal content on video-sharing platforms, as well as for small-scale and niche sources, such as online platforms for the distribution of game videos; this draught intends to include such providers within its ambit. Additionally, many provisions of German penal law prohibit the statement or broadcast of false or untrue personal information.

### *6.12.3 Brazil*

If intermediaries are needed to monitor content, the growth of new services via innovation may be inhibited, so producing a 'permission-first culture. Brazil's Federal Government and civil society worked to produce progressive laws in response to the Azeredo Bill. The establishment of the Marco Civil da Internet required multi-stakeholder engagement and a constitutional component through fundamental recognition. The right to freedom of speech guarantees an unfettered capacity for information transmission and reception. To preserve a fair playing field and net neutrality, access is required. Individual's privacy and data security are increased by giving them control over their information.

Due process guarantees that the law takes priority over arbitrariness, and legal procedure assures justice and impartiality via the rights to be informed of the law, to obtain notice of an alleged offence, and to a reasoned decision. Without being bound by proprietary technologies or other rigid legal procedures, a free and open internet may be realized via 'permission-less innovation.

### *6.12.4 South Korea*

Since 1995, South Korea's Information & Communication Ethics Office has been authorised by law to order information providers to delete or restrict content that "violates public morals," results in a violation of the nation's sovereignty, or is information that may harm the character, emotions, and sense of value of youths.

---

<sup>48</sup>Sally Broughton Micova, 'The Audiovisual Media Services Directive', *Research Handbook on EU Media Law and Policy* (2021).

### *6.12.5 People's Republic of China*

As is the case in other countries, the default pre-safe-harbor position under Chinese law is that intermediaries with sufficient knowledge of infringing activity affecting their services would be held jointly and severally liable.

The intermediary liability system for defamation in China is neither rigid nor a genuine safe harbor; rather, it is constrained in the sense that intermediaries are only responsible for unlawful content of which they are aware. Rather of adopting an exemption rule (e.g., Shall not be responsible for unknown or legal material,)<sup>49</sup> China created a liability rule that imposes obligation for either (a) known unlawful content or (b) unlawful content informed by a third party.

### *6.12.6 United States of America*

The Communications Decency Act, 1996<sup>50</sup>, shields intermediaries and social media platforms from liability for hosting third-party material. Former U.S. President Trump recently ordered the repeal of Section 230 after accusing Twitter of bias towards conservative political ideals<sup>51</sup>.

Additionally, they have the Child Online Privacy Protection Act, 1998<sup>52</sup>, which empowers them to delete anything that is detrimental to non-adult users, however this was deemed unconstitutional; nonetheless, hosting any unlawful content remains prohibited. This statute's principal objective is to offer parents control over the information obtained online concerning their young children.

After analyzing the legality of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 and comparing them to various international laws

---

<sup>49</sup>Yuan Virtanen, Asta Salmi and Xiao Qin, 'Modern Mediators: Intermediaries' Informational Roles in Sourcing from China' (2021) *Journal of Business and Industrial Marketing* 654.

<sup>50</sup>Brent G Paterson and Rodney J Peterson, 'The Communications Decency Act of 1996' [1996] *ACM SIGUCCS Newsletter*.

<sup>51</sup>Ellen P Goodman and Ryan Whittington, 'Section 230 of the Communications Decency Act and the Future of Online Speech' (2019) *SSRN Electronic Journal* 506.

<sup>52</sup>Berin Michael Szoka and Adam D Thierer, 'COPPA 2.0: The New Battle Over Privacy, Age Verification, Online Safety & Free Speech' (2011) *SSRN Electronic Journal* 33.



regulating social media and digital media, I can conclude that these rules appear hastily enacted to curtail free speech, a malafide attempt to dominate the online space, and in desperate need of judicial review. The Supreme Court said that the IT Rules, 2021 lack teeth due to the absence of a clause compelling intermediaries to adhere to the rules.

On the other hand, the case studies demonstrate that, although social media companies claim to have followed the central government's recommendations, they have actively sought to disrupt the process. While the legislation mandates human action and the designation of a grievance officer for Facebook, Twitter, and Instagram, the social media giants have resorted to merely posting the officer's name and email address, but the answers users get are automated. In essence, big IT is duping the government into thinking that the regulations are being adhered to.

## **CHAPTER 7**

### **CONCLUSION AND SUGGESTION**

#### **7.1 INTRODUCTION**

More than 120 nations have already enacted some type of international privacy rules for data protection, ensuring that individuals and their data are provided with more stringent safeguards and restrictions. It is evident that international privacy rules for data protection will continue to change and improve to assure the protection of personal data across all use cases and scenarios, even some that have not yet occurred.

In general, the worldwide privacy rules for data protection adhere to or are influenced by the following five global privacy principles:

1. Notification entails notifying users, visitors, readers, and users of the policies in place to protect their personal data.
2. Choice and consent entails providing people with alternatives and permission about the acquisition, use, storage, and management of their personal data.
3. Access and participation entails ensuring that the proper persons have access to the information and use it in compliance with the necessary security measures.
4. Integrity and security entails ensuring that the data are secure, and that unauthorised access is impossible.
5. Compliance enforcement entails ensuring that a service, website, solution, and platform adhere to a regulation that mandates compliance.

#### **7.2 What are the advantages of global privacy regulation?**

In 2018, the General Data Protection Regulation (GDPR) became the most comprehensive and forward-thinking legal instrument for the protection and ongoing security of personal data. This

is an international privacy regulation for data protection that applies to any organisation that processes any personal data (including biometric data) of an EU citizen.<sup>1</sup>

It set the standard and inspired the prevalent trends in this field today. The ultimate goal of data protection is to safeguard data and information from internal and external threats. It secures the individual by decreasing the probability of fraud, compromise, and corruption.

As the amount of data collected and stored continues to expand exponentially, increased data security has become vital and necessary. This has had an impact on global data protection policy and has the following benefits:

- Valuable data is secured against disclosure, loss, and theft
- Businesses may enhance public, investor, and consumer confidence
- Brand value is intrinsic and implied in a solid policy and structure.
- Effective corporate governance enhances a firm's competitive advantage
- Improvements in automation, digitization, and innovation owing to the transformation of business processes
- Enhanced reliability and trustworthiness across numerous markets and consumers
- Greater comprehension of the data, its worth, and the advantages it provides
- Improved data management and control leading to enhanced innovation and transformation

### **7.3 Most well-known Data Protection Regulation**

The legislation governing the protection of personal data vary considerably from area to region and even nation to country. Some places, such as Europe, have implemented tight restrictions that inflict hefty penalties on rule-breakers, while others, such as the United States, continue to grapple with formal and centralised laws that provide unified protection. GDPR enforcement

---

<sup>1</sup>Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) Information and Communications Technology Law 76.

resulted in a seismic change in how governments, organisations, and people regarded data privacy and a swift transition toward more stringent regulations and safeguards.

Here are a few of the most prominent locations and nations with worldwide privacy rules for data protection:

- Europe – The GDPR law was less of a localised security and compliance measure and more of an international privacy rule for data protection that applied to any organisation that processed the personal data of any EU citizen. Today, with the global implementation of security and data protection measures, the future of data protection will be marked by stricter rules, harsher fines, and more reputational damage if compliance is ignored. After some companies violated the GDPR and were hit with substantial fines, corporations took note. The execution of the General Data Protection Regulation (GDPR) and the resulting costly penalties and reputational harm have placed organisations in a difficult situation. They must be compliant, and they need the proper assistance to do so<sup>2</sup>.
- The United States – while there are no official laws at the federal level, there is some basic federal legislation that safeguards data. As a consequence of the devolution of power to the state level, a number of states in the United States have implemented their own data-related laws. The California Consumer Privacy Act (CCPA), which guarantees significant privacy rights and consumer protection, is considered one of California's most progressive legislations.<sup>3</sup>. The legislation permits state citizens to choose exactly how and why their personal information is gathered and used. Other states have enacted or pending legislation include Alabama, Connecticut, Florida, New York, Washington, Illinois, Texas, and Virginia. The current state of the United States' privacy laws may be found here.
- The General Data Protection Law of Brazil supports and complements the more than 40 data privacy-related laws passed over the years. This legislation resolves contradictions between many laws, defines personal data and public data, clarifies clear liabilities, and applies to all sectors of the country. This law also demands the employment of Data Protection Officers, the

---

<sup>2</sup>Thomas Linden and others, 'The Privacy Policy Landscape After the GDPR' (2020) Proceedings on Privacy Enhancing Technologies 84.

<sup>3</sup>Derek Lackey and Neil Beaton, 'The Current State of Data Protection and Privacy Compliance in Canada and the USA' (2019) Applied Marketing Analytics 334.

execution of high security requirements, and the enhancement of security measures to ensure comprehensive compliance. The Lei Geral de Proteco de Dados (LGPD) of Brazil entered into effect on September 18, 2017 and sets a legal framework for the use of personal data of Brazilian people regardless of the location of the data processor. In spite of this, its administrative sanctions were enforced in August 2021, making this year a test run for how the National Data Protection Authority (ANPD) would implement the LGPD.<sup>4</sup>

- South Africa has enacted the Protection of Personal Information Act (POPIA) with equally strict and stringent requirements for the protection of personal data. Since it was first proposed in 2013, the Act has undergone several amendments and adjustments, and its final layers are expected to be finalised in July 2021. The privacy standards and protections outlined in the POPIA are equivalent to those in the GDPR.<sup>5</sup>

- The Data Protection Law of Bahrain is the first of its kind to be established in the Middle East; it offers individuals rights surrounding the collecting, processing, and storage of personal information.

- The Data Privacy Act of 2012 in the Philippines has a lot of the features that define the EU Data Protection Directive and guarantees the protection of personal data by organisations. The Canadian government implemented the Personal Information Protection and Electronic Documents Act (PIPEDA), which is compatible with EU data protection laws. The Act is very compliant with the five worldwide privacy standards and offers strong protection for the personal information of consumers. The Digital Charter Implementation Act (DCIA) was proposed by the Canadian Minister of Information, Science, and Economic Development on November 17, 2020. If passed, this measure would replace PIPEDA and introduce various unique changes to the nation's privacy regulations. This contains a private right of action and potential penalties beyond those of the GDPR. This was examined again in 2021.

- The GDPR was applicable in the United Kingdom until July 31, 2021, after which alternative legislation took effect due to Brexit. Nevertheless, the Data Protection Act of 2018 has already

---

<sup>4</sup>Abigayle Erickson, 'Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD' (2019) Brooklyn Journal of International Law 128.

<sup>5</sup>Anneliese Roos, 'The European Union's General Data Protection Regulation (GDPR) and Its Implications for South African Data Privacy Law: An Evaluation of Selected Content Principles (2021) Comparative and International Law Journal of Southern Africa 97.

incorporated the obligations of the EU's GDPR into British law as of January 1, 2021. The Data Protection, Privacy, and Electronic Communications (DPPEC) Regulations of 2019 replaced the Data Protection Act (DPA) of 2018 with the General Data Protection Regulation (GDPR) to create a comprehensive, UK-specific data protection system that applies within the UK context and is known as the UK GDPR.

#### 7.4 Data Protection Law in India

In 2019 government brought the personal data protection bill. After discussion in Lok Sabha and Rajya Sabha this bill was referred to joint parliamentary committee. As per the JPC recommendations a lot of changes were suggested by JPC in the bill<sup>6</sup>. On August 3, 2022, the center withdrew the personal data protection bill that it had tabled in Lok Sabha on December 11th, 2019. The bill which had undergone intense scrutiny by a JPC would now be replaced by a new bill that fits into the comprehensive legal framework as per the government statement on the withdrawal.

the JPC 542-page report has 93 recommendations 81 amendments and suggested 97 corrections and improvements to the bill. One of the key recommendations is widening the ambit of the bill to cover all data instead of just personal data<sup>7</sup>.

The stated view of government is that in face of such a radical overhaul it is better to bring a new bill.

##### *7.4.1 Timeline Of the Bill*

- The Justice Sri Krishna panel was established in 2017 in response to the Supreme Court's ruling that privacy is a basic right and its directive to the government to develop a national data protection framework.

---

<sup>6</sup>Dvara Research, 'Comments to the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill 2019 Introduced in the Lok Sabha on 11 December 2019' (2020) SSRN Electronic Journal 43.

<sup>7</sup>Dr Anusuya Yadav and Gaurav Yadav, 'Data Protection in India in Reference to Personal Data Protection Bill 2019 and IT Act 2000' (2021) IARJSET 67.

- In the same year, the Sri Krishna committee published a white paper defining the scope of their investigation.
- In July of 2018, the committee submitted a draught of a data protection law to the ministry of electronics and information technology, which said that it will develop a new statute based on the concepts outlined in the Sri Krishna committee report.
- The measure was sent to the Joint Parliamentary Committee in December 2019.

#### *7.4.2 Recommendations by the Committee*

- The joint parliamentary committee submitted its report in November 2021 clearing clause 35, the provision that enables government agencies to bypass provision of the law citing “public order”“sovereignty”, “friendly relations with foreign states” and “security of state”.
- The opposition members of the JPC submitted strong dissent votes along with the report.
- The JPC tabled its report after 78 sitting spreads over 184 hours and 20 minutes.
- It recommended 81 revisions to the finished draught, along with 12 suggestions, such as increasing the proposed law's scope to include discussion of non-personal data, so shifting the bill's mission from data protection to wider data protection.
- The JPC study also advised modifications to concerns such as social media company regulation and the use of only trustworthy hardware in cellphones, etc. It was recommended that social media businesses that do not operate as intermediaries by authenticating users' profiles should be considered content creators and held responsible for the material they host.
- Data fiduciary must be mandated to report every personal data breach in specific circumstances within 72 hours.
- Selection committee for DPA should include Attorney General, independent experts and directors off IIT/ IIM.
- Certification of digital devices.
- Policy on data localization.

The research suggested following:

### **7.5 Research Objectives**

- To analyse whether implementation of Data protection laws in India based on GDPR (General Data Protection Regulation) (E.U), where the socio-economic conditions of both the regions are entirely different, the fundamental right of privacy has different effect altogether, will prove to be an effective data protection regime.
- To examine whether the current situation of social networking websites, and the consent regulation followed by them is capable enough to protect individual rights.
- To study the data protection laws of other democracies specially Singapore and U.S.A and understand the way they have enforced data privacy for the citizens of their country.
- To understand how the bill if not withdrawn would have increased data protection obligations significantly.
- To make a comparative analysis of various provisions related to privacy under GDPR and Data Protection Bill, 2021.

**7.6 HYPOTHESIS** of the study is that *Implementation of Data Protection Laws in India, which is influenced by GDPR (General Data Protection Regulation) will protect the fundamental right to privacy and is a practical approach, to preserve individual rights, increase government transparency and strengthen data privacy regime.*

*In-depth research and critical analysis have proven the hypothesis to be “Null and void”.*

With the bill being withdrawn we are back to the situation where there is no specific bill or act dealing with data protection law in India and therefore the practical protection of right to privacy with reference to data protection is questionable.

The reasons for the withdrawal and the problems with policy are as follows:

- The current IT laws mandates notice and permission for data collection and imposes additional important requirements on data processing. As they are founded on ideas for



the control of data (fair information practises) developed before the present market structure, it is possible that they do not effectively guarantee privacy. Additionally, they do not shield users against losses resulting from a breach of privacy. These requirements may enhance moral hazard and cause consumers to overestimate the advantages of privacy legislation.

- Second, the law lacks any empirical grasp of the trade-offs consumers make when submitting information. The Srikrishna committee<sup>8</sup>, which created the first version of the law, did not conduct research to determine the circumstances in which users are prepared to give personal information for advantages. According to evidence from other countries, these trade-offs vary based on the circumstances of the transaction. Insofar as the law protects privacy without providing proof of its relevance to users, it might have a detrimental impact on the advantages of data-driven innovation without successfully safeguarding personal data.
- Third, the term "harms" was not well defined. Many of these harms are intrinsic to a variety of business choices. The bill's notion of damage might have considerably altered corporate regulation without providing privacy protection.
- Fourth, the government's ability to exclude government entities from the law for surveillance purposes constituted a new and independent authority to acquire personal data. It is unclear why this provision was necessary, and the bill failed to provide sufficient checks and balances on the exercise of these powers.
- The Data Protection Authority's design was marred by structural flaws. The bill's expansive preventative architecture imposed severe capacity limits. The proposed authority composition did not allow for independent input or supervision.
- The consent age of child was fixed to 18 years. The consent age of children should be based on graded approach.

These challenges highlight a need for a more realistic and restrained approach to data protection and the damages caused by the abuse of data. The bill was more state centric in its ability to

---

<sup>8</sup>Justice B.N. Srikrishna, 'White Paper of the Committee of Experts on a Data Protection Framework for India' (2017) White Paper PL 108.

control organisations that gather data and provided the state with more monitoring tools. There were clear limitations to the effectiveness of this regulation architecture in preserving privacy. Instead, the framework should carefully and precisely concentrate on issues that may be handled effectively by legislation.

### **7.7 Following Suggestions have Emerged from This Research:**

It is evident that without permission, data should not be collected and used. Businesses that breach this concept would also be in violation of Indian constitutional informational privacy norms and user property rights. Additionally, consenting individuals must be permitted to accept responsibility for their decisions. In most consumer-oriented industries, regulation consists of establishing whether certain contractual conditions and practises are unfair, deceptive, or misleading to customers. The emphasis of the law should shift from enforcing preventative responsibilities to identifying and regulating such activities and terms in data-sharing agreements. The existing legal regime does not effectively safeguard users from certain injuries and damages that may be incurred. People and society should be safeguarded from damage caused by a breach of data privacy, such as discrimination on constitutionally protected grounds, identity manipulation, financial theft, fraud, and threats to national sovereignty and integrity. This attention must be given to the reformulation of damages clauses.

The Ministry of Electronics and Information Technology and the courts must provide the National Technical Research Organisation, the National Intelligence Grid, and the National Information Board with strong policy, legislative, and infrastructural support so that they can perform their duties effectively. The Data Protection Bill 2021, as presented to the Indian parliament, was not a comprehensive data protection framework for India. The major concern was that the Bill did not strike a perfect balance between the privacy of citizens and the need for occasional government intervention, it was likely that, if enacted, the Bill would have never served as an effective means of data protection (and the protection of related interests, such as free speech) than current legislation.

Despite India's efforts to build and create data protection and privacy regulations, there are still certain gaps that need to be addressed. Consequently, our Indian legislature must include the

positive aspects of data protection and privacy legislation from across the globe and take a step ahead in the adoption and development of this new branch of law, given its utmost relevance in the modern day. There are several data protection regulations throughout the globe that, if enacted and rigorously followed in India, might help to reduce data protection-related difficulties.

The Data Protection Bill 2021 is the best illustration of how data-driven policy has altered law enforcement, as legislators must now consider the technological era in which we live and make laws that can address the newly emerging needs and problems, such as cyber-crime, social media bullying, privacy breach, and data hoarding.

The public data makes us more vulnerable because, if it falls into the wrong hands, it can pose a significant threat to our freedom and lead to an increase in antisocial and criminal behaviour, which can be used as a weapon in the future by individuals for personal gain or by other nations to further their own agendas. Due to the reliance of society on computerised systems for everything from air traffic control to medical care to national security, even a little glitch in these operations might imperil our lives.

The notion of property encompasses data protection regulations since, in the cyber world, data is the basis of our property-specific legal measures and a component of our right to ownership. The measure was inadequate to address the privacy-related harms of India's data economy. Consequently, this area of law is evolving in India, and it is anticipated that it will soon be handled.

It is also suggested that the regulatory ambiguity must be minimised to provide business certainty. The bill had several regulatory ambiguities. First, it lacked an adequate definition of sensitive personal data. Second, it did not provide approval standards for cross-border data transfers. Thirdly, it granted the government the authority to demand the exchange of non-personal data without stipulations about the use of this authority or the payment of compensation.

Further that the authority granted to the government to exclude any government agency from the obligations of the law should be balanced by the inclusion of suitable protections in the measure

itself. The government should not have the authority to choose which agencies are exempt and which protections apply to such institutions.

Any new authority to data protection should consider India's state capacity restrictions. The nature of the data economy will make it almost difficult to adequately govern data processing. The extent of that authority's mission should be rationalised by the other recommendations presented here. For instance, the authority would lose the jurisdiction to restrict the right to access, the right to be forgotten, and other rights. Any such authority and the government should make decisions via a very participatory procedure. This is far more relevant in this instance than for other regulators due to the cross-sector application of the bill's requirements. Accordingly, the new law should authorise the government and the Authority to undertake a comprehensive consultation process for the creation of all rules, regulations, and codes of conduct.

The Telecom Regulatory Authority of India, the Airports Economic Regulatory Authority, and the Insolvency and Bankruptcy Board of India, among others, engage in extensive consultations prior to drafting rules. Therefore, it is suggested that the new law should guarantee that the data protection authority adopts the best practises for drafting rules and codes of practise.

Despite India's efforts to build and create data protection and privacy regulations, there are still certain gaps that need to be addressed. Consequently, our Indian legislature must include the positive aspects of data protection and privacy legislation from across the globe and take a step ahead in the adoption and development of this new branch of law, given its utmost relevance in the modern day. There are several data protection regulations throughout the globe that, if enacted and rigorously followed in India, might help to reduce data protection-related difficulties.

## **7.8 Future ahead**

India is set to implement a wave of data and information technology legislation changes after more than a decade of inaction. The change will undoubtedly assist India in realising its true potential as one of the world's most powerful data-driven economies. The Indian government may begin developing a new law to replace the Information Technology Act of 2000 in the near

future ("IT Act"). As part of this process, it seems that the government may enact guidelines on data governance and cybersecurity, a "Digital India Act" to replace the IT Act, and new legislation to replace the Personal Data Protection Bill ("PDP Bill").

The ill-fated PDP Bill, which has undergone many amendments by a Joint Parliamentary Committee since 2018, including a short stint as the "Data Protection Bill 2021," has been scrapped in order to be recreated from start, forcing us to return to the drawing board. The PDP Bill offered a number of problematic concepts, including data localisation and data mirroring, which caused tremendous concern among corporate actors who would have been compelled to reorganise significant sections of their data flow systems to comply with such requirements. The existing IT Act is an anachronism and does not appropriately meet modern data protection needs. Therefore, a comprehensive revision of all data legislation in India is a step towards a comprehensive solution to India's data challenges.

Changes in data- and technology-related regulations are not exclusive to India. Recently, stringent data protection regulations such as the EU GDPR, California's CCPA, and China's Personal Information Protection Law have become the norm, with each nation vigorously protecting the privacy of personal data. All of these laws have been adopted during the last decade. Countries throughout the world are presently attempting to implement the requirements of these laws into their data flow networks in order to protect both economic and individual rights. US President Joe Biden and European Commission President Ursula von der Leyen announced coordinated efforts to build a new EU-US data-sharing framework that will enhance / replace the existing EU-US Privacy Shield in March 2022. The recent Schemes I and II decisions by the Court of Justice of the European Union nullified the current Privacy Shield as a result of surveillance regulations in the United States exposing EU citizen data, thereby introducing uncertainty regarding data transfers between the European Union and the United States. Any measure that mandates the global localisation of all data without equivalent safeguards for foreign data risks breaking EU standards and a number of other national data laws.

The upcoming adjustments to India's data protection laws, in whatever form they may take, must be cognizant of the changing global data protection environment. The recent "Data Accessibility and Use Policy" of the Government of India, which was withdrawn practically immediately after

it was announced, seems to miss the mark on this problem by focusing entirely on the commercialization of enormous data sets.

Any new legislation passed by the Indian government must take into consideration a number of essential factors. First, the law should require businesses and government agencies in India to implement a "privacy-by-design" policy, in which the default way for storing personal data is to empower data principals with total control over data privacy, as well as a set of opt-out options. Second, strict security measures should be a precondition for the monetization of data. Elements such as data localisation, categorization of data types, cross-border data flow and storage should be regulated with company operations and individual rights in mind. Complementary regulations should explain aspects like regulatory processes, logistics, data centres, and internet connectivity.

India is one of the few countries lacking a comprehensive, modern data protection legislative framework. In view of India's desire to project a global image of a digital economy with a flourishing data services industry, the Government must immediately develop a structure that aligns it with its overseas counterparts. Unlike other laws, data protection legislation cannot work domestically in isolation and must be consistent with the international arena.

# REFERENCES

## 1. PRIMARY SOURCES

### 1.1 LIST OF CASES

#### INTERNATIONAL CASES

SNO.	NAME OF THE CASE	PAGE NUMBER
1.	Douglas vs. Hello Ltd. (2005) EWCA Civ. 595	49,50
2.	Duchess of Argyll vs. Duke of Argyll 1967 Ch 302	48
3.	Grisworld vs. Conecticut 381 U.S. 479 (1965)	33
4.	Nuth Mull vs. Zuka-Oollah Beg Sr.D.A.N.W.P.R 1855	76
5.	PG and JH vs. United Kingdom (App 44787/98) (2008) 46 EHRR 51	31
6.	Prince Albert vs. Strange 41 ER 1171	77
7.	Von Hannover vs. Germany (2004) (App 59320/00)	31

#### INDIAN CASES

SNO.	NAME OF THE CASE	PAGE NUMBER
1.	M.P. Sharma &Ors. vs. Satish Chandra 1954 AIR 300, 1954 SCR 1077	2,4
2.	Kharak Singh Case 1963 AIR 1295, 1964 SCR (1) 332	2,4,20,38,42
3.	People's Union for Civil Liberties Case AIR 1997 SC 568	3,20,39,72
4.	K.S. Puttaswamy (Retd.) vs. Union of India AIR 2017 SC 4161	3,8,17,20,37,40,69,70,71,1 36,173
5.	R.Rajagopal vs. State of T.N. 1994 AIR 264, 1994 SCC (6) 632	20,39,42,43
6.	Gobind vs. State of Madhya Pradesh 1975 (2) SCC 14	3,20,38,42
7.	Unique Identification Authority of India &Anr. vs. Central Bureau of Investigation	21,25,40
8.	Selvi&Ors. vs. State of Karnataka AIR 2010 SC 1974	23,40
9.	Maneka Gandhi vs. Union Of India 1978 AIR 597	37
10.	District Registrar Collector, Hyderabad &Anr. Vs. Canara Bank &Anr. AIR 2005 SC 186	39
11.	Sahara India Real Estate Corpn. Ltd. vs. SEBI (2013) 1 SCC 1	43
12.	KeshoSahu vs. MusammatMuktakiman	45
13.	M. Gurudas vs. Rasaranjan AIR 2006 SC 3275	49
14.	Amar Singh vs. Union of India (2011) 7 SCC 69	50
15.	Navtej Singh Johar and ors vs. Union of India and Ors (2018) 10 SCC 1	70,74
16.	Joseph Shine vs. Union of India AIR 2018 SC 4898	71
17.	Association of Indian Young lawyers and ors. vs. The	71

	State of Kerala and Ors. (2019) 11 SCC 1	
18	Vinit Kumar vs. Central Investigation Bureau and Ors	72
19	Central Public Information Officer Supreme Court vs. Subhash Chandra Agarwal 2019 SCC OnLine SCC 1459	73
20	NALSA vs. Union of India AIR 2014 SC 1863	73
21	Association of Indian Hotels and Restaurants (AHAR) and Ors. vs. The State of Maharashtra AIR 2019 SC 589	74
22	Avnish Bajaj vs. State (NCT of Delhi) 116 (2005) DLT 427	288
23	Shreya Singhal vs. Union of India (2013) 12 SCC 73	290

## **1.2 STATUTES**

### **1.2.1 INTERNATIONAL STATUTES**

1. Act on Protection of Personal Information, Japan 2005.
2. Bundesdatenschutzgesetz (BDSG), Germany 1990.
3. Children's Online Privacy Protection Act, USA 1998.
4. Data Privacy Act, Philippines 2012.
5. Datenschutzgesetz (DSG), Austria 2000.
6. Federal Act on Data Protection, Switzerland 1992.
7. French Data Protection Act, 2018.
8. General Data Protection Regulation, European Union 2016.
9. Law on Personal Data Protection of Montenegro, Spain 2018.
10. Lei Geral de Protecao de Dados Pessoais, Brazil 2020.
11. Privacy Act, Australia 1988.
12. The Federal Law on the Protection of Personal Data held by Private Parties, Mexico 2010.
13. The Personal Data (Privacy) Ordinance, Hongkong 1996.
14. UNCITRAL, Model Law on Electronic Commerce Guide to Enactment (2001).

### **1.2.2 NATIONAL STATUTES**

1. The Indian Easement Act, 1882
2. The Information Technology Act, 2000
3. The Reserve Bank of India Act, 1934
4. The Code of Criminal Procedure, 1973
5. The Constitution of India, 1950
6. The Indian Penal Code, 1860



7. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

## 2. SECONDARY SOURCES

### 2.1 BOOKS

1. Alexander P, *Information Security: A Manager's Guide to Thwarting Data Thieves and Hackers*, (Praeger 2008)
2. Barnes R, *Outrageous Invasions: Celebrities' Private Lives, Media, and the Law*, (Oxford University Press Publication New York 2010).
3. Barry E, *Privacy in the 21st Century*, (Libraries Unlimited 2005)
4. Basu P, *Law Relating to Protection of Human Rights under the Indian Constitution and Allied Laws*, (Modern Law Publications New Delhi 2007).
5. Bennett and Colin J, *The Governance of Privacy: Policy Instruments in Global Perspective*, (Ashgate Publication, Hampshire, England, 2003).
6. Brown and Geoffrey, *The Information Game: Ethical Issues in a Microchip World*, (Humanities Press International, Inc. Publication, New Jersey, U.S.A & London, U.K., 1st ed. 1990).
7. Burdon M, *Digital Data Collection, and Information Privacy Law*, (Cambridge University Press, 2020).
8. Carey and Peter, *Media Law*, (Sweet & Maxwell Ltd. Publication, London 5th ed. 2010).
9. Chandra U, *Human Rights* (Allahabad Law Agency Publications, Allahabad, 5th ed. 2004).
10. Clayton and Richard, *Privacy and Freedom of Expression* (Oxford University Press Publication New York 2010).
11. Deshta and Kiran, *Right to Privacy under Indian Law*, (Deep & Deep Publications Pvt. Ltd., New Delhi, 2011).
12. Gilbar and Roy, *The Status of the Family in Law and Bioethics: The Genetic Context*, (Ashgate Publication, Hampshire, England, 2005).
13. Gross and Hyman, *Privacy: Its Legal Protection*, (Oceana Publications, Inc. Dobbs Ferry, New York, U.S.A., Revised ed. 1976).
14. Henry and Michael, *International Privacy, Publicity & Personality Laws*, (Butterworths Publications, U.K., (ed.), 2001).

15. Hoffman and Lance J., *Modern Methods for Computer Security and Privacy*, (Prentice Hall Inc. Publication, Englewood Cliffs, New Jersey, U.S.A., 1977).
16. Hoofnagle C, *Federal Trade Commission Privacy Law, and Policy* (Cambridge University Press, New York, 2016).
17. Hull L and Charles P, *Roe v. Wade: The Abortion Rights Controversy in American History*, (University Press of Kansas Publication, U.S.A., 2001).
18. Hyde S and Montgomery H, *Privacy, and the Press: The Daily Mirror Photographer Libel Action*, (Butterworth & Co. Publication, London, (ed.), 1947).
19. Irvine D, *Human Rights, Constitutional Law and the Development of the English Legal System* (Hart Publishing 2003)
20. Jain M. P., *Indian Constitutional Law*, (Wadhwa and Company, Nagpur, 5th ed. Reprint, 2005).
21. Kennedy C and Alderman E, *The Right to Privacy* (Knopf 1996)
22. Kenyon, Andrew R and Megan, *New Dimensions in Privacy Law: International and Comparative Perspectives*, (Cambridge University Press Publication, Cambridge 2006).
23. Kuschewsky M, *Data Protection and Privacy: Jurisdictional Comparisons*, (Sweet & Maxwell Ltd. Publication, London 2012).
24. Lyon D, *Surveillance Studies: An Overview*, (Polity Press Publication, Cambridge U.K 2007).
25. Madgwick D, *The Invasion of Privacy*, (Pitman Publishing Corporation, New York, U.S.A., 1st ed. 1974).
26. Martin J, *Security, Accuracy and Privacy in Computer Systems*, (Prentice Hall Inc. Publication, Englewood Cliffs, New Jersey, 1973).
27. Michael J, *Privacy and Human Rights*, (UNESCO Publishing, Paris, France and Dartmouth Publishing Co. Ltd., Hampshire, England, 1994).
28. Miller and Arthur R, *The Assault on Privacy*, (Ann Arbor, Michigan University Press, 1971).
29. Arthur M, *The Assault on Privacy: Computers, Data Banks, and Dossiers*, (The University of Michigan Press Publication, U.S.A., 1971).
30. Mishra G, *Right to Privacy in India*, (Preeti Publications, Delhi, 1st ed. 1994).
31. Barrington J, *Privacy: Studies in Social and Cultural History*, (M.E. Sharpe Inc. Publication, New York, 1984).

32. Nagel T, *Concealment and Exposure: And Other Essays*, (Oxford University Press Publication, New York, 2002).
33. Catrien H, *E-Discovery, and Data Privacy: A Practical Guide*, (Wolters Kluwer Law & Business Publication, 2011).
34. Brien O and David M, *Privacy, Law, and Public Policy*, (Praeger Publishers Publication, New York, 1979).
35. Pandey J. N., *Constitutional Law of India*, (Central Law Agency, Allahabad, 40th ed. 2003).
36. Pember and Don R, *Privacy & The Press* (University of Washington Press Publication, U.S.A., 2nd Reprint, 1972).
37. Richards N, *Intellectual Privacy-Rethinking Civil Liberties in The Digital Age*, (Oxford University Press, 2015).
38. Robertson A, *Privacy and Human Rights*, (MUP, Manchester, 1972).
39. Schonberger M, *The Virtue of Forgetting in The Digital Age*, (Princeton University Press, 2009).
40. Sharma, S, *Privacy Law: A Comparative Study*, (Atlantic Publishers and Distributors, New Delhi, 1994).
41. Simons G, *Privacy in the Computer Age*, (NCC Publications, Manchester, England, 1982).
42. Solove, Daniel J, Paul M and others, *Privacy, and the Media*, (Aspen Publishers, New York, 2008).
43. Solove D, Paul M, and others, *Privacy Information and Technology*, (Wolters Kluwer Law & Business Publication, New York, 3rd ed. 2011).
44. Swire P, and Ahmad K, *Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws, and Practices*, (International Association of Privacy Professionals, Portsmouth, 2012).
45. Toulson R and Phipps C, *Confidentiality*, (Sweet & Maxwell Ltd. Publication, London, 2nd ed. 2006).
46. Vincete D, *Data Protection on The Internet*, (Springer 2020).
47. Wacks and Raymond, *The Protection of Privacy*, (Sweet & Maxwell Ltd. Publication, London, 1980).
48. Waldo J and Herbert L, *Engaging Privacy and Information in A Digital Age*, (The Academies Press, 2007).

49. Westin and Alan F, *Privacy and Freedom*, (Atheneum Publication, New York, 1970).
50. Yeeffen H, *Data Protection in The Practical Context*, (Academy Publishing, 2017).

## 2.2 ARTICLES

### 2.2.1 ARTICLES OF INDIAN JOURNALS

1. Adithan V “Right to Privacy under Article 21” (2003) Madras Law Journal Vol. I PL 11.
2. Ahmad M “Muslim Law and Reforms: Protection of Privacy in Islam” (2000) Civil and Military Law Journal Vol. 36 PL 73.
3. Awasthi S “Privacy Laws in India: Big Brother is Watching You” (2002) Company Law Journal Vol. 3 PL 49.
4. Bajwa D “Right to Privacy – its Origin & Ramifications” (1990) Civil & Military Law Journal Vol. 26 PL 66.
5. Bhandari M “Right to Privacy Versus Freedom of Press: A Comparative Conspectus of Legal Position in U.S.A., U.K. and India” (1991) The Indian Journal of Legal Studies, Vol. XI PL 47.
6. Bharuka D “Piercing the Privacy Veil: A renewed threat” (2003) Supreme Court Cases Vol.1 PL 77.
7. Deshta S “Right to Privacy: An Extension of Personal Liberty” (2005) M.D.U. Law Journal, Vol. X (1) PL 7.
8. Goswami K and Dhruv. “Right to Privacy: In the Perspective of the Information Technology Act, 2000” (2005) Gauhati Law Times, Vol. II PL 98.
9. Gupta S and Misra P. “Right to Privacy – An Analysis of Developmental Process in India, America and Europe” (2005) Central India Law Quarterly, Vol.18 PL 81.
10. Gupta S “Right to Privacy is an Aspect of Human Dignity”, Journal of Legal Studies” (1985) Vol. 17, PL 31.
11. Iyer K “Privacy is Human Right” (1990), Press Council of India Review, Vol.11, PL 117.
12. Jain R “The Right to Privacy and Freedom of Information: The Search for a Balance” (1979) Indian Journal of Public Administration, Vol.25 (4) PL 49.
13. Jathin E “Human Genome Project: Emerging Challenges of Right to Privacy vis-à-vis Insurer’s Right to Know” (2007) Cochin University Law Review, Vol. XXXI PL 87.

14. Jayashree L “Right to Privacy of a Woman under Criminal Law” (2003) Criminal Law Journal Vol.109 PL 69.
15. Joshi K “Right to Privacy: An Extension of Personal Liberty” (1978) Kurukshetra Law Journal, Vol. 4 PL 89.
16. Lal S “Human Rights and Right to Privacy: In Historical and Present Perspectives” Journal of the Legal Studies (2006) Vol. XXXVII PL 69.
17. Lekshmi G “Electronic Surveillance – A Tool for Invasion of Privacy”, The Academy Law Review (2008) Vol.32 PL 117.
18. Noorani A “Privacy vs. Public Interest” (2001) Press Council of India Review, Vol.22, PL 201.
19. Noorani A “Right to Privacy” (2005) Economic and Political Weekly Vol.40 (9) PL 57.
20. Parikh S “Right to Privacy” (1984) Civil and Military Law Journal, Vol. 20 PL 67.
21. Pati S “Right to Privacy: Whether Fundamental?” (2000) Indian Bar Review, Vol. 27 PL 9.
22. Patnaik P “HIV/AIDS Victim’s Right to Privacy” (1999) Cuttack Law Times, Vol.88 PL 114.
23. Pattnaik N and Nanda S “Legal Aspects of Pre-Natal Diagnostic Technique” (2005) Central India Law Quarterly, Vol. 18 PL 34.
24. Pillai N and Ramnath K “Trumping Public Interest: Should Violation of Privacy be a Tort?” (2006) Cochin University Law Review, Vol. XXX PL 66.
25. Prasad A “New Dimensions of the Right of Privacy under the Indian Constitution” (1980) Journal of Constitutional & Parliamentary Studies Vol. 4 PL10.
26. Qadri S and Afzal M “Women and Law relating to Sex Determination Test: With Special Reference to J & K State” (2008) Kashmir University Law Review, Vol. XIV PL 77.
27. Reddy C “Piety of Privacy after Death” (1991) Lawyers Collective, Vol.6 PL 16.
28. Reddy S “Right to Privacy of Parties in Matrimonial Disputes – An Analysis” (2005) Andhra Law Times, Vol.1 PL 15.
29. Revathi R “Pervasive Technology, Invasive Privacy and Lucrative Piracy – A Critique” (2009) Journal of the Indian Law Institute Vol.51(3) PL 34.
30. Sivakumar S “Right to Privacy” (1994) The Academy Law Review, Vol.18 PL 67.
31. Sorabjee S “Privacy and Defamation: SC Defines Parameters” (1995) Press Council of India Review Vol. 16 PL 114.

32. Tageldin, M and Rahman A “Right to Privacy and Abortion: A Comparative Study of Islamic and Western Jurisprudence” (1997) Aligarh Law Journal Vol. XII, PL 106.
33. Upadhyay M. L. and Jayaswal P “Constitutional Control of Right to Privacy” (1989) Central India Law Quarterly, Vol. 2 PL 133.

### **2.2.2 ARTICLES OF FOREIGN JOURNALS**

1. Bamberger L, Kenneth A., and Mulligan K “Privacy on the Books and on the Ground” (2011) Stanford Law Review Vol.63 (2) PL 148.
2. Benjamin K “Fictions of Privacy: House Chapels and the Spatial Accommodation of Religious Dissent in Early Modern Europe” (2002) American Historical Review Vol.107 (4) PL 97.
3. Bradford L and Kathleen L “A Stress Test for Privacy, the GDPR and Data Protection Regimes” (2020) Journal of Law, and Bio sciences Vol. 33 PL 25.
4. Bratman B “Brandeis and Warren’s The Right to Privacy and the Birth of the Right to Privacy” (2002) Tennessee Law Review Vol. 7 PL 344.
5. Christina P “Moving from Nixon to NASA: Privacy ‘s Second Strand- A Right to Informational Privacy” (2012) Yale Journal of Law and Technology Vol. 76 PL 154.
6. Connor N and Lange A “Privacy in the Digital Age” (2015) Great Decisions Vol. 6 PL 17.
7. Derek M “Beyond Toleration: Privacy, Citizenship and Sexual Minorities in England and Wales” (2004) British Journal of Sociology Vol.55 (3) PL 38.
8. Diane P “The moral value of informational privacy in cyberspace” (2001) Ethics and Information Technology Vol 3 PL 129.
9. Donald H “A Matter of Privacy: Managing Personal Data in Company Computers” (1987) Personnel Law Journal Vol.64 (2) PL 67.
10. Edward L “The Right to be Forgotten v. Free Speech” (2015) Journal of Law, and Policy for the Information Society Vol. 29 PL 103.
11. Erwin C “Rediscovering Right to Privacy” (2007) Brandeis Law Journal, Vol.45 (4), PL 188.
12. Francesca B “Case for Tolerant Constitutional Patriotism: The Right to Privacy before the European Courts” (2008) Cornell International Law Journal Vol.41 (2) PL 607.

13. Loring B “Analysis of the Informational Privacy Protection afforded by the European Union and the United States” (2002) *Texas International Law Journal* Vol.37 (2) PL 55.
14. Margulis S “On the Status and Contribution of Westin’s and Altman’s Theories of Privacy” (2003) *Journal of Social Issues*, Vol.59 (2) PL 68.
15. Mendelson S and Morrison K “The Right to Privacy in the Workplace: Testing Applicants for Alcohol and Drug Abuse” (1988) *Personnel Law Journal* Vol.65(8) PL 108.
16. Michael C “A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe” (2014) *Connecticut Journal of International Law* Vol. 8PL 261.
17. Moira P and Maeve M Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data (2018) *Monash University Law Review* Vol. 21 PL 44.
18. Mun-Cho K “Surveillance Technology, Privacy and Social Control: With Reference to the Case of the Electronic National Identification Card in South Korea” (2004) *International Sociology* Vol.19 (2) PL 234.
19. Anthony P “Designing for Democracy: Does the Personal Data Protection Bill 2019 Champion Citizen Rights?” (2020) *Economic and Political Weekly* Vol. 55 PL 21.
20. Priscilla M “Privacy, Government, Information and Technology” (1986) *Public Administration Review* Vol.46 (6) PL 143.
21. Richard P “Privacy, Surveillance, and Law” (2008) *University of Chicago Law Review* Vol. 67PL 245.
22. Sanford L “Public Lives and the Limits of Privacy” (1988) *Political Science and Politics* Vol.21 (2) PL156
23. Schermer B “The crisis of consent: how stronger legal protection may lead to weaker consent in data protection” (2014) *Ethics and Information Technology* Vol.5 PL 213.
24. Schwartz P and Solove D “Reconciling personal information in the United States and European Union” (2014) *California Law Review* Vol. 39PL 877.
25. Smith H “Information Privacy and Marketing: What the US should (and shouldn’t) learn from Europe” (2001) *California Management Review*, Vol.43 (2) PL 67.
26. Solove D and Hartzog W “The FTC and the new common law of privacy” (2014) *Colum Law Review* Vol. 17 PL 583.

27. Terry N, “Existential challenges for health care data protection in the United States”, Ethics Med Public Health Vol 8 PL 19.
28. Warren S and Brandeis L “The Right to Privacy” (1890) Harvard Law Review Vol. 4 PL 193.
29. Weber R “The right to be forgotten More than a Pandora's Box” (2011) Journal of Intellectual Property Information Technology and E-commerce Vol. 3 PL 120.
30. Wong B “The journalism exception in UK data protection law” (2020) Journal of Media Law Vol. 43 PL 216.

### **2.2.3 CONVENTIONS**

1. African Charter of Human and People’s Rights, 1981
2. African Charter on the Rights and Welfare of the Child, 1990
3. American Convention on Human Rights ,1967
4. American Convention on Human Rights, 1969
5. Convention on the Rights of Child, 1989
6. Convention on the Rights of Persons with Disabilities, 2007
7. European Convention on Human Rights, 1950
8. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990
9. International Covenant on Civil and Political Rights, 1966

### **2.2.4 ONLINE SOURCES**

1. ‘Australian Government- Federal Register of Legislation’ <https://www.legislation.gov.au/Details/C2021C00242> accessed on 22 July 2021.
2. A free and fair digital economy, protecting privacy, empowering Indians ‘Committee of Experts under the Chairmanship of Justice B.N. Srikrishna’ 114, [https://www.meity.gov.in/writereaddata/files/Data\\_Protection\\_Committee\\_Report.pdf](https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf) accessed on 27 August 2021.



3. ACCC ‘Digital Platforms Inquiry, Final Report’ 462, <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf> accessed on 2 March 2022.
4. African Charter on the Rights and Welfare of the Child, [https://au.int/sites/default/files/treaties/36804-treatyafrican\\_charter\\_on\\_rights\\_welfare\\_of\\_the\\_child.pdf](https://au.int/sites/default/files/treaties/36804-treatyafrican_charter_on_rights_welfare_of_the_child.pdf) , accessed on 4 September 2021.
5. Alessandro A ‘The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines’ in *Joint WPISP-WPIE Roundtable* OECD, 2010 <https://www.oecd.org/sti/ieconomy/46968784.pdf>, accessed on 28 April 2021.
6. Barbaschow A ‘Australian privacy law amendments to cover data collection and use by digital platforms’ (2020) <https://www.zdnet.com/article/australian-privacy-law-amendment-to-cover-data-collection-and-use-by-digital-platforms/> accessed on 22 March 2021.
7. Basu A and Sherman J ‘Key Global Takeaways From India's Revised Personal Data Protection Bill. Lawfare’ <https://www.lawfareblog.com/key-global-takeaways-indias-revised-personal-data-protection-bill> accessed on 23 September 2021.
8. Bhandari, V, Kak and Parsheera, ‘An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict’ <https://www.indrastra.com/2017/11/An-Analysis-of-Puttaswamy-Supreme-Court-s-Privacy-Verdict-003-11-2017-0004.html> accessed on 29 July 2021.
9. Big Data: Seizing Opportunities and Preserving Values, Executive Office of the President, May 2014, [https://obamawhitehouse.archives.gov/sites/default/files/docs/big\\_data\\_privacy\\_report\\_may\\_1\\_2014.pdf](https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf) accessed on 10 July 2021.
10. Burman A ‘Will India’s Data Protection Law Protect Privacy and Promote Growth?’ (2020), [https://carnegieendowment.org/files/Burman\\_Data\\_Privacy.pdf](https://carnegieendowment.org/files/Burman_Data_Privacy.pdf) , accessed on 27 January 2021.
11. CAN-SPAM Act: ‘A Compliance Guide for Business, Federal Trade Commission’ <https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guidebusiness> accessed on 25 August 2021.
12. Cathy N ‘Big Data Algorithms are Manipulating Us’ WIRED, <https://www.wired.com/2016/10/big-data-algorithms-manipulating-us/> -accessed on 18 May 2020.

13. Cravigan E ‘In a nutshell: data protection, privacy and cybersecurity in Australia’(October 2020) Lexology, <https://www.lexology.com/library/detail.aspx?g=2027ba56-6178-4e7f-9273-9aa9bb2f5066> accessed on 11 December 2021.
14. Directive 95/46/EC, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046> accessed on 6 October 2021.
15. Doyle C “Privacy: an overview of the Electronic Communications Privacy Act” Congressional Research Service, <https://www.hsdl.org/?view&did!4725508> accessed on 16 November 2021.
16. Erik S ‘People Are Concerned About Their Privacy in Theory, Not Practice, Says New Study’ Fortune <https://fortune.com/2019/02/25/consumers-data-privacy/> 25 February 2020,
17. Jasmine A ‘Privacy in Cyber Space Livelaw’ <https://www.livelaw.in/columns/privacy-in-cyber-space-157769> accessed on 3 February 2021)
18. Kashmir Hill ‘Revenge Porn with A Facebook Twist’ Forbes. <https://www.forbes.com/sites/kashmirhill/2011/07/06/revenge-porn-with-a-facebook-twist/?sh=4393773b1d2e> accessed on 17 November 2020.
19. Mathew R ‘Personal Data Protection Bill, 2019 –Examined through the Prism of Fundamental Right to Privacy – A Critical Study’ [https://www.sconline.com/blog/post/2020/05/22/personal-data-protection-bill-2019-examined-through-the-prism-of-fundamental-right-to-privacy-a-critical-study/#\\_ftn26](https://www.sconline.com/blog/post/2020/05/22/personal-data-protection-bill-2019-examined-through-the-prism-of-fundamental-right-to-privacy-a-critical-study/#_ftn26) accessed on 22 May 2020.
20. Morris M and Cravigan E ‘The Privacy, Data Protection and Cyber Security Law Review- Australia’ <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/australia> accessed on 13 April 2021.
21. Patel N and Jain A ‘Government to Enhance Data Privacy and to ‘Regulate the Digital Age’ [https://www.gcllegal.com.au/limelight-newsletters/government-to-enhance-data-privacy-and-protection-to-regulate-the-digital-age/?utm\\_source=Mondaq&utm\\_medium=syndication&utm\\_campaign=LinkedIn-integration](https://www.gcllegal.com.au/limelight-newsletters/government-to-enhance-data-privacy-and-protection-to-regulate-the-digital-age/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration) accessed on 18 March 2022.
22. Privacy Act 1988, <https://www.legislation.gov.au/Details/C2014C00076> accessed on 22 May 2021.

23. Robert H ‘Data Protection Law In USA’ Advocates for International Development, [https://www.neighborhoodindicators.org/sites/default/files/course-materials/A4ID\\_DataProtectionLaw%20.pdf](https://www.neighborhoodindicators.org/sites/default/files/course-materials/A4ID_DataProtectionLaw%20.pdf) accessed on 23 November 2021.
24. Rosen J, ‘The Right to be Forgotten’ Symposium Issue, Stanford Law Review Online (2012) <https://review.law.stanford.edu/wp-content/uploads/sites/3/2012/02/64-SLRO-88.pdf> accessed on 22 August 2021.
25. Salinas S and Meredith S ‘Personal data collection is being ‘weaponized against us with military efficiency’<https://www.cnbc.com/2018/10/24/apples-tim-cook-warns-silicon-valley-it-would-be-destructive-to-block-strong-privacy-laws.html> accessed on 11 June 2021
26. Schermer B, Custers B, and Simone H ‘The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection’(2014) *Ethics and Information Technology*<https://link.springer.com/article/10.1007/s10676-014-9343-8> accessed on 22 February 2020.
27. Sinha A ‘Right to be Forgotten – A Tale of two Judgments’ Centre for Internet Society <https://cis-india.org/internet-governance/blog/right-to-be-forgotten-a-tale-of-two-judgments>, accessed on 18 April 2021
28. Steven P ‘What is Big Data? More than Volume, Velocity and Variety...IBM Developer Blog’ (2017). <https://developer.ibm.com/blogs/what-is-big-data-more-than-volume-velocity-and-variety/>accessed on 06 July 2021.
29. Watts D and Casanovas P, ‘Privacy and Data Protection in Australia: a Critical overview’ (extended abstract) <https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf> accessed on 25 September 2021.

### **2.2.5 REPORTS**

1. A free and fair digital economy, protecting privacy, empowering Indians, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Pg-114, [https://www.meity.gov.in/writereaddata/files/Data\\_Protection\\_Committee\\_Report.pdf](https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf) accessed on 23 September 2020.
2. Report of the Group of Experts on Privacy Constituted by Planning Commission of India under the Chairmanship of Justice A.P Shah, Former Chief Justice, Delhi High Court,

<https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf>  
accessed on 21 July 2021.

# **Right to Privacy and Data Protection Laws in India: Balancing Rights and Managing Conflicts**

*Thesis submitted in fulfilment of the requirements for the Degree of*

**DOCTOR OF PHILOSOPHY**

By

**Sumedha Ganjoo**



**BENNETT**  
**UNIVERSITY**  
A TIMES GROUP INITIATIVE

Department of School of Law

**BENNETT UNIVERSITY**

(Established under UP Act No 24, 2016)

Plot Nos 8-11, Tech Zone II,

Greater Noida-201310, Uttar Pradesh, India.

Month- July Year- 2022

## **CHAPTER 7**

### **CONCLUSION AND SUGGESTION**

#### **7.1 INTRODUCTION**

More than 120 nations have already enacted some type of international privacy rules for data protection, ensuring that individuals and their data are provided with more stringent safeguards and restrictions. It is evident that international privacy rules for data protection will continue to change and improve to assure the protection of personal data across all use cases and scenarios, even some that have not yet occurred.

In general, the worldwide privacy rules for data protection adhere to or are influenced by the following five global privacy principles:

1. Notification entails notifying users, visitors, readers, and users of the policies in place to protect their personal data.
2. Choice and consent entails providing people with alternatives and permission about the acquisition, use, storage, and management of their personal data.
3. Access and participation entails ensuring that the proper persons have access to the information and use it in compliance with the necessary security measures.
4. Integrity and security entails ensuring that the data are secure, and that unauthorised access is impossible.
5. Compliance enforcement entails ensuring that a service, website, solution, and platform adhere to a regulation that mandates compliance.

#### **7.2 What are the advantages of global privacy regulation?**

In 2018, the General Data Protection Regulation (GDPR) became the most comprehensive and forward-thinking legal instrument for the protection and ongoing security of personal data. This

is an international privacy regulation for data protection that applies to any organisation that processes any personal data (including biometric data) of an EU citizen.<sup>1</sup>

It set the standard and inspired the prevalent trends in this field today. The ultimate goal of data protection is to safeguard data and information from internal and external threats. It secures the individual by decreasing the probability of fraud, compromise, and corruption.

As the amount of data collected and stored continues to expand exponentially, increased data security has become vital and necessary. This has had an impact on global data protection policy and has the following benefits:

- Valuable data is secured against disclosure, loss, and theft
- Businesses may enhance public, investor, and consumer confidence
- Brand value is intrinsic and implied in a solid policy and structure.
- Effective corporate governance enhances a firm's competitive advantage
- Improvements in automation, digitization, and innovation owing to the transformation of business processes
- Enhanced reliability and trustworthiness across numerous markets and consumers
- Greater comprehension of the data, its worth, and the advantages it provides
- Improved data management and control leading to enhanced innovation and transformation

### **7.3 Most well-known Data Protection Regulation**

The legislation governing the protection of personal data vary considerably from area to region and even nation to country. Some places, such as Europe, have implemented tight restrictions that inflict hefty penalties on rule-breakers, while others, such as the United States, continue to grapple with formal and centralised laws that provide unified protection. GDPR enforcement

---

<sup>1</sup>Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) Information and Communications Technology Law 76.

resulted in a seismic change in how governments, organisations, and people regarded data privacy and a swift transition toward more stringent regulations and safeguards.

Here are a few of the most prominent locations and nations with worldwide privacy rules for data protection:

- Europe – The GDPR law was less of a localised security and compliance measure and more of an international privacy rule for data protection that applied to any organisation that processed the personal data of any EU citizen. Today, with the global implementation of security and data protection measures, the future of data protection will be marked by stricter rules, harsher fines, and more reputational damage if compliance is ignored. After some companies violated the GDPR and were hit with substantial fines, corporations took note. The execution of the General Data Protection Regulation (GDPR) and the resulting costly penalties and reputational harm have placed organisations in a difficult situation. They must be compliant, and they need the proper assistance to do so<sup>2</sup>.
- The United States – while there are no official laws at the federal level, there is some basic federal legislation that safeguards data. As a consequence of the devolution of power to the state level, a number of states in the United States have implemented their own data-related laws. The California Consumer Privacy Act (CCPA), which guarantees significant privacy rights and consumer protection, is considered one of California's most progressive legislations.<sup>3</sup>. The legislation permits state citizens to choose exactly how and why their personal information is gathered and used. Other states have enacted or pending legislation include Alabama, Connecticut, Florida, New York, Washington, Illinois, Texas, and Virginia. The current state of the United States' privacy laws may be found here.
- The General Data Protection Law of Brazil supports and complements the more than 40 data privacy-related laws passed over the years. This legislation resolves contradictions between many laws, defines personal data and public data, clarifies clear liabilities, and applies to all sectors of the country. This law also demands the employment of Data Protection Officers, the

---

<sup>2</sup>Thomas Linden and others, 'The Privacy Policy Landscape After the GDPR' (2020) Proceedings on Privacy Enhancing Technologies 84.

<sup>3</sup>Derek Lackey and Neil Beaton, 'The Current State of Data Protection and Privacy Compliance in Canada and the USA' (2019) Applied Marketing Analytics 334.



execution of high security requirements, and the enhancement of security measures to ensure comprehensive compliance. The Lei Geral de Proteção de Dados (LGPD) of Brazil entered into effect on September 18, 2017 and sets a legal framework for the use of personal data of Brazilian people regardless of the location of the data processor. In spite of this, its administrative sanctions were enforced in August 2021, making this year a test run for how the National Data Protection Authority (ANPD) would implement the LGPD.<sup>4</sup>

- South Africa has enacted the Protection of Personal Information Act (POPIA) with equally strict and stringent requirements for the protection of personal data. Since it was first proposed in 2013, the Act has undergone several amendments and adjustments, and its final layers are expected to be finalised in July 2021. The privacy standards and protections outlined in the POPIA are equivalent to those in the GDPR.<sup>5</sup>

- The Data Protection Law of Bahrain is the first of its kind to be established in the Middle East; it offers individuals rights surrounding the collecting, processing, and storage of personal information.

- The Data Privacy Act of 2012 in the Philippines has a lot of the features that define the EU Data Protection Directive and guarantees the protection of personal data by organisations. The Canadian government implemented the Personal Information Protection and Electronic Documents Act (PIPEDA), which is compatible with EU data protection laws. The Act is very compliant with the five worldwide privacy standards and offers strong protection for the personal information of consumers. The Digital Charter Implementation Act (DCIA) was proposed by the Canadian Minister of Information, Science, and Economic Development on November 17, 2020. If passed, this measure would replace PIPEDA and introduce various unique changes to the nation's privacy regulations. This contains a private right of action and potential penalties beyond those of the GDPR. This was examined again in 2021.

- The GDPR was applicable in the United Kingdom until July 31, 2021, after which alternative legislation took effect due to Brexit. Nevertheless, the Data Protection Act of 2018 has already

---

<sup>4</sup>Abigail Erickson, 'Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD' (2019) Brooklyn Journal of International Law 128.

<sup>5</sup>Anneliese Roos, 'The European Union's General Data Protection Regulation (GDPR) and Its Implications for South African Data Privacy Law: An Evaluation of Selected Content Principles (2021) Comparative and International Law Journal of Southern Africa 97.

incorporated the obligations of the EU's GDPR into British law as of January 1, 2021. The Data Protection, Privacy, and Electronic Communications (DPPEC) Regulations of 2019 replaced the Data Protection Act (DPA) of 2018 with the General Data Protection Regulation (GDPR) to create a comprehensive, UK-specific data protection system that applies within the UK context and is known as the UK GDPR.

#### 7.4 Data Protection Law in India

In 2019 government brought the personal data protection bill. After discussion in Lok Sabha and Rajya Sabha this bill was referred to joint parliamentary committee. As per the JPC recommendations a lot of changes were suggested by JPC in the bill<sup>6</sup>. On August 3, 2022, the center withdrew the personal data protection bill that it had tabled in Lok Sabha on December 11th, 2019. The bill which had undergone intense scrutiny by a JPC would now be replaced by a new bill that fits into the comprehensive legal framework as per the government statement on the withdrawal.

the JPC 542-page report has 93 recommendations 81 amendments and suggested 97 corrections and improvements to the bill. One of the key recommendations is widening the ambit of the bill to cover all data instead of just personal data<sup>7</sup>.

The stated view of government is that in face of such a radical overhaul it is better to bring a new bill.

##### *7.4.1 Timeline Of the Bill*

- The Justice Sri Krishna panel was established in 2017 in response to the Supreme Court's ruling that privacy is a basic right and its directive to the government to develop a national data protection framework.

---

<sup>6</sup>Dvara Research, 'Comments to the Joint Parliamentary Committee (JPC) on the Personal Data Protection Bill 2019 Introduced in the Lok Sabha on 11 December 2019' (2020) SSRN Electronic Journal 43.

<sup>7</sup>Dr Anusuya Yadav and Gaurav Yadav, 'Data Protection in India in Reference to Personal Data Protection Bill 2019 and IT Act 2000' (2021) IARJSET 67.

- In the same year, the Sri Krishna committee published a white paper defining the scope of their investigation.
- In July of 2018, the committee submitted a draught of a data protection law to the ministry of electronics and information technology, which said that it will develop a new statute based on the concepts outlined in the Sri Krishna committee report.
- The measure was sent to the Joint Parliamentary Committee in December 2019.

#### *7.4.2 Recommendations by the Committee*

- The joint parliamentary committee submitted its report in November 2021 clearing clause 35, the provision that enables government agencies to bypass provision of the law citing “public order”“sovereignty”, “friendly relations with foreign states” and “security of state”.
- The opposition members of the JPC submitted strong dissent votes along with the report.
- The JPC tabled its report after 78 sitting spreads over 184 hours and 20 minutes.
- It recommended 81 revisions to the finished draught, along with 12 suggestions, such as increasing the proposed law's scope to include discussion of non-personal data, so shifting the bill's mission from data protection to wider data protection.
- The JPC study also advised modifications to concerns such as social media company regulation and the use of only trustworthy hardware in cellphones, etc. It was recommended that social media businesses that do not operate as intermediaries by authenticating users' profiles should be considered content creators and held responsible for the material they host.
- Data fiduciary must be mandated to report every personal data breach in specific circumstances within 72 hours.
- Selection committee for DPA should include Attorney General, independent experts and directors off IIT/ IIM.
- Certification of digital devices.
- Policy on data localization.

The research suggested following:

### **7.5 Research Objectives**

- To analyse whether implementation of Data protection laws in India based on GDPR (General Data Protection Regulation) (E.U), where the socio-economic conditions of both the regions are entirely different, the fundamental right of privacy has different effect altogether, will prove to be an effective data protection regime.
- To examine whether the current situation of social networking websites, and the consent regulation followed by them is capable enough to protect individual rights.
- To study the data protection laws of other democracies specially Singapore and U.S.A and understand the way they have enforced data privacy for the citizens of their country.
- To understand how the bill if not withdrawn would have increased data protection obligations significantly.
- To make a comparative analysis of various provisions related to privacy under GDPR and Data Protection Bill, 2021.

**7.6 HYPOTHESIS** of the study is that *Implementation of Data Protection Laws in India, which is influenced by GDPR (General Data Protection Regulation) will protect the fundamental right to privacy and is a practical approach, to preserve individual rights, increase government transparency and strengthen data privacy regime.*

*In-depth research and critical analysis have proven the hypothesis to be “Null and void”.*

With the bill being withdrawn we are back to the situation where there is no specific bill or act dealing with data protection law in India and therefore the practical protection of right to privacy with reference to data protection is questionable.

The reasons for the withdrawal and the problems with policy are as follows:

- The current IT laws mandates notice and permission for data collection and imposes additional important requirements on data processing. As they are founded on ideas for

the control of data (fair information practises) developed before the present market structure, it is possible that they do not effectively guarantee privacy. Additionally, they do not shield users against losses resulting from a breach of privacy. These requirements may enhance moral hazard and cause consumers to overestimate the advantages of privacy legislation.

- Second, the law lacks any empirical grasp of the trade-offs consumers make when submitting information. The Srikrishna committee<sup>8</sup>, which created the first version of the law, did not conduct research to determine the circumstances in which users are prepared to give personal information for advantages. According to evidence from other countries, these trade-offs vary based on the circumstances of the transaction. Insofar as the law protects privacy without providing proof of its relevance to users, it might have a detrimental impact on the advantages of data-driven innovation without successfully safeguarding personal data.
- Third, the term "harms" was not well defined. Many of these harms are intrinsic to a variety of business choices. The bill's notion of damage might have considerably altered corporate regulation without providing privacy protection.
- Fourth, the government's ability to exclude government entities from the law for surveillance purposes constituted a new and independent authority to acquire personal data. It is unclear why this provision was necessary, and the bill failed to provide sufficient checks and balances on the exercise of these powers.
- The Data Protection Authority's design was marred by structural flaws. The bill's expansive preventative architecture imposed severe capacity limits. The proposed authority composition did not allow for independent input or supervision.
- The consent age of child was fixed to 18 years. The consent age of children should be based on graded approach.

These challenges highlight a need for a more realistic and restrained approach to data protection and the damages caused by the abuse of data. The bill was more state centric in its ability to

---

<sup>8</sup>Justice B.N. Srikrishna, 'White Paper of the Committee of Experts on a Data Protection Framework for India' (2017) White Paper PL 108.

control organisations that gather data and provided the state with more monitoring tools. There were clear limitations to the effectiveness of this regulation architecture in preserving privacy. Instead, the framework should carefully and precisely concentrate on issues that may be handled effectively by legislation.

### **7.7 Following Suggestions have Emerged from This Research:**

It is evident that without permission, data should not be collected and used. Businesses that breach this concept would also be in violation of Indian constitutional informational privacy norms and user property rights. Additionally, consenting individuals must be permitted to accept responsibility for their decisions. In most consumer-oriented industries, regulation consists of establishing whether certain contractual conditions and practises are unfair, deceptive, or misleading to customers. The emphasis of the law should shift from enforcing preventative responsibilities to identifying and regulating such activities and terms in data-sharing agreements. The existing legal regime does not effectively safeguard users from certain injuries and damages that may be incurred. People and society should be safeguarded from damage caused by a breach of data privacy, such as discrimination on constitutionally protected grounds, identity manipulation, financial theft, fraud, and threats to national sovereignty and integrity. This attention must be given to the reformulation of damages clauses.

The Ministry of Electronics and Information Technology and the courts must provide the National Technical Research Organisation, the National Intelligence Grid, and the National Information Board with strong policy, legislative, and infrastructural support so that they can perform their duties effectively. The Data Protection Bill 2021, as presented to the Indian parliament, was not a comprehensive data protection framework for India. The major concern was that the Bill did not strike a perfect balance between the privacy of citizens and the need for occasional government intervention, it was likely that, if enacted, the Bill would have never served as an effective means of data protection (and the protection of related interests, such as free speech) than current legislation.

Despite India's efforts to build and create data protection and privacy regulations, there are still certain gaps that need to be addressed. Consequently, our Indian legislature must include the

positive aspects of data protection and privacy legislation from across the globe and take a step ahead in the adoption and development of this new branch of law, given its utmost relevance in the modern day. There are several data protection regulations throughout the globe that, if enacted and rigorously followed in India, might help to reduce data protection-related difficulties.

The Data Protection Bill 2021 is the best illustration of how data-driven policy has altered law enforcement, as legislators must now consider the technological era in which we live and make laws that can address the newly emerging needs and problems, such as cyber-crime, social media bullying, privacy breach, and data hoarding.

The public data makes us more vulnerable because, if it falls into the wrong hands, it can pose a significant threat to our freedom and lead to an increase in antisocial and criminal behaviour, which can be used as a weapon in the future by individuals for personal gain or by other nations to further their own agendas. Due to the reliance of society on computerised systems for everything from air traffic control to medical care to national security, even a little glitch in these operations might imperil our lives.

The notion of property encompasses data protection regulations since, in the cyber world, data is the basis of our property-specific legal measures and a component of our right to ownership. The measure was inadequate to address the privacy-related harms of India's data economy. Consequently, this area of law is evolving in India, and it is anticipated that it will soon be handled.

It is also suggested that the regulatory ambiguity must be minimised to provide business certainty. The bill had several regulatory ambiguities. First, it lacked an adequate definition of sensitive personal data. Second, it did not provide approval standards for cross-border data transfers. Thirdly, it granted the government the authority to demand the exchange of non-personal data without stipulations about the use of this authority or the payment of compensation.

Further that the authority granted to the government to exclude any government agency from the obligations of the law should be balanced by the inclusion of suitable protections in the measure

itself. The government should not have the authority to choose which agencies are exempt and which protections apply to such institutions.

Any new authority to data protection should consider India's state capacity restrictions. The nature of the data economy will make it almost difficult to adequately govern data processing. The extent of that authority's mission should be rationalised by the other recommendations presented here. For instance, the authority would lose the jurisdiction to restrict the right to access, the right to be forgotten, and other rights. Any such authority and the government should make decisions via a very participatory procedure. This is far more relevant in this instance than for other regulators due to the cross-sector application of the bill's requirements. Accordingly, the new law should authorise the government and the Authority to undertake a comprehensive consultation process for the creation of all rules, regulations, and codes of conduct.

The Telecom Regulatory Authority of India, the Airports Economic Regulatory Authority, and the Insolvency and Bankruptcy Board of India, among others, engage in extensive consultations prior to drafting rules. Therefore, it is suggested that the new law should guarantee that the data protection authority adopts the best practises for drafting rules and codes of practise.

Despite India's efforts to build and create data protection and privacy regulations, there are still certain gaps that need to be addressed. Consequently, our Indian legislature must include the positive aspects of data protection and privacy legislation from across the globe and take a step ahead in the adoption and development of this new branch of law, given its utmost relevance in the modern day. There are several data protection regulations throughout the globe that, if enacted and rigorously followed in India, might help to reduce data protection-related difficulties.

## **7.8 Future ahead**

India is set to implement a wave of data and information technology legislation changes after more than a decade of inaction. The change will undoubtedly assist India in realising its true potential as one of the world's most powerful data-driven economies. The Indian government may begin developing a new law to replace the Information Technology Act of 2000 in the near



future ("IT Act"). As part of this process, it seems that the government may enact guidelines on data governance and cybersecurity, a "Digital India Act" to replace the IT Act, and new legislation to replace the Personal Data Protection Bill ("PDP Bill").

The ill-fated PDP Bill, which has undergone many amendments by a Joint Parliamentary Committee since 2018, including a short stint as the "Data Protection Bill 2021," has been scrapped in order to be recreated from start, forcing us to return to the drawing board. The PDP Bill offered a number of problematic concepts, including data localisation and data mirroring, which caused tremendous concern among corporate actors who would have been compelled to reorganise significant sections of their data flow systems to comply with such requirements. The existing IT Act is an anachronism and does not appropriately meet modern data protection needs. Therefore, a comprehensive revision of all data legislation in India is a step towards a comprehensive solution to India's data challenges.

Changes in data- and technology-related regulations are not exclusive to India. Recently, stringent data protection regulations such as the EU GDPR, California's CCPA, and China's Personal Information Protection Law have become the norm, with each nation vigorously protecting the privacy of personal data. All of these laws have been adopted during the last decade. Countries throughout the world are presently attempting to implement the requirements of these laws into their data flow networks in order to protect both economic and individual rights. US President Joe Biden and European Commission President Ursula von der Leyen announced coordinated efforts to build a new EU-US data-sharing framework that will enhance / replace the existing EU-US Privacy Shield in March 2022. The recent Schemes I and II decisions by the Court of Justice of the European Union nullified the current Privacy Shield as a result of surveillance regulations in the United States exposing EU citizen data, thereby introducing uncertainty regarding data transfers between the European Union and the United States. Any measure that mandates the global localisation of all data without equivalent safeguards for foreign data risks breaking EU standards and a number of other national data laws.

The upcoming adjustments to India's data protection laws, in whatever form they may take, must be cognizant of the changing global data protection environment. The recent "Data Accessibility and Use Policy" of the Government of India, which was withdrawn practically immediately after

it was announced, seems to miss the mark on this problem by focusing entirely on the commercialization of enormous data sets.

Any new legislation passed by the Indian government must take into consideration a number of essential factors. First, the law should require businesses and government agencies in India to implement a "privacy-by-design" policy, in which the default way for storing personal data is to empower data principals with total control over data privacy, as well as a set of opt-out options. Second, strict security measures should be a precondition for the monetization of data. Elements such as data localisation, categorization of data types, cross-border data flow and storage should be regulated with company operations and individual rights in mind. Complementary regulations should explain aspects like regulatory processes, logistics, data centres, and internet connectivity.

India is one of the few countries lacking a comprehensive, modern data protection legislative framework. In view of India's desire to project a global image of a digital economy with a flourishing data services industry, the Government must immediately develop a structure that aligns it with its overseas counterparts. Unlike other laws, data protection legislation cannot work domestically in isolation and must be consistent with the international arena.