A COMPARATIVE PERSPECTIVE ON DATA PROTECTION LAWS – WITH REFERENCE TO EUROPE, UNITED STATES OF AMERICA, THE UNITED KINGDOM AND INDIA

A THESIS SUBMITTED IN PARTIAL FULFILLMENT FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN THE MANOHAR PARRIKAR SCHOOL OF LAW, GOVERNANCE & PUBLIC POLICY

GOA UNIVERSITY

By

Mr. Amonkar Vassudev Anant Sinai

V.M. Salgaocar College of Law, Research Centre, Miramar.

MAY, *2023*

DECLARATION

I, **Mr. Amonkar Vassudev Anant Sinai** hereby declare that this thesis entitled, **"A Comparative Perspective on Data Protection Laws – With Reference to Europe, United States Of America, The United Kingdom and India",** represents work which has been carried out by me and that it has not been submitted, either in part or full, to any other University or Institution for the award of any research degree.

Place: Miramar, Goa.

Date : 23-05-2023 **Amonkar Vassudev Anant Sinai**

CERTIFICATE

I hereby certify that the work was carried out under my supervision and may be placed for evaluation.

Dr. Nagesh S. Colvalkar
Research Guide
V.M. Salgaocar College of Law, Miramar, Goa.

ACKNOWLEDGMENTS

There is a famous saying, **"*Knowledge is in the end, based on acknowledgment*"**. I am obligated to so many distinct individuals in the preparation of this research study that I may probably not be able to mention every single one of them individually. Though it is worthwhile to recognise and acknowledge certain gems without whom the research study would have been an enigmatic fantasy.

As an expression of gratitude, I would like to begin by expressing my deepest appreciation and gratitude to my research guide, **Dr. Nagesh S.Colvalkar**, Ex-Associate Professor at V.M. Salgaocar College of Law, and now, Member Judge at Goa State Consumer Redressal Commission and Author of *Criminal Administration: Law and Practice,* who has been instrumental in encouraging me to start my research on this area of study. His effective inputs and guidance at every stage of the research work has been extremely beneficial to me. He graciously made it relatively simple for me to traverse this path. Sir, I remain ever grateful to you.

Special gratitude is due to the members of the Departmental Research Committee, **Prof Dr. V Sudesh**, Chairperson, University Law College & Dept. Of Studies, Bangalore University, Bengaluru and **Dr. Shaber Ali. G**, Off. Principal, V.M. Salgaocar College of Law for their invaluable and indispensable assistance, recommendations, steady support, motivation, and most importantly, direction and suggestions in guiding me to complete my research thesis on time.

I am deeply indebted to **Dr. M.R.K Prasad**, Professor of Law, V.M. Salgaocar College of Law**, Dr. Saba V.M.Da Silva**, Professor and Principal, GR Kare College of Law, **Dr. K.Srinivasa Rao**, Associate Professor, V.M. Salgaocar College of Law, **Dr. B.S.Patil**, Associate Professor, V.M. Salgaocar College of Law, **Dr.Sandhya Ram**, Associate Professor, V.M. Salgaocar College of Law and **Dr.Andryusha Pinho**. The people who were always there for discussions on

anything that I was unsure of and who have offered invaluable advice that will benefit me throughout my life.

I am grateful to **Shri. Anand R. Salve,** Librarian (Sr.Scale), GR Kare College of Law, **Shri. Nandkishor K. Bandekar**, Asst. Librarian, Goa University and **Shri. Nalin Faldessai**, College Librarian, V.M. Salgaocar College of Law for their patience and valuable assistance.

I would also like to extend my sincere thanks to **Mrs. Rupam V.Korgaonkar**, Office Staff, V.M. Salgaocar College of Law, **Ms. Divyata Khandeparkar**, Office Assistant, Academic Section Goa University, **Mr. Kshitij Naik**, LDC, Examination Section, Goa University, **Mr.Vishwas B. Bhairaokar**, **Mr. Anand C. Naik and Mr. Ramakant P. Naik,** Library Staff**,** V.M. Salgaocar College of Law, for their continued support and encouragement.

Last but not the least, words cannot express my gratitude to my parents **late Dr.Ananta V.S.Amonkar** and **late Usha A.S.Amonkar,** who could not get to see me complete my thesis. Thank You for believing in me and for the insightful conversations we've had along the way. I would also like to express my immense gratitude to my sister **Ms. Pranali A.S.Amonkar**, who has been very understanding and patient and most importantly gave me my space and time to help me achieve this milestone .Thank you for keeping me sane.

I would like to thank all the people who contributed in some way to the work described in this thesis and who positively have helped me in so many ways to bring this work into its final shape.

May God continue to bless you all.

Amonkar Vassudev Anant Sinai

"Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet."

– Gary Kovacs[1]

[1] Gary Kovacs, Brainy Quote, available at: https://www.brainyquote.com/authors/gary-kovacs-quotes (Last accessed on March 15, 2023).

TABLE OF CONTENTS

MODE OF CITATION

As the legal profession is diverse and rapidly changing, *The Bluebook* maintains a uniform standard of citations in order to communicate important information as well as the sources and legal authorities on which they rely in their research work. Over passage of time, legal researchers, students of law, advocates, scholars, Judges, and other legal professionals have relied on *The Bluebook's* unique citation system in their writings.

The Researcher has followed **"The Bluebook: A Uniform System of Citation, Harvard Law Review Association," 17th edition, 2004,** standards in the citations, in this thesis.

ABBREVIATIONS

Aadhaar Act	The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016
AI	Artificial Intelligence
AIR	All India Reporter
APEC	Asia-Pacific Economic Cooperation
Apps	Application
ARPU	Average Revenue Per User
BHIM	Bharat Interface for Money
BLAPL	Bail Application
BREXIT	It is the name given to the United Kingdom's departure from the European Union. It is a combination of 'Britain' and 'exit'.
Bom	Bombay
CalOPPA	California Online Privacy Protection Act, 2004
CAN-SPAM	Non-Solicited Pornography and Marketing Act,2003
CBI	Central Bureau of Investigation
CCPA	The California Consumer Privacy Act, 2018
CCTV	Closed Circuit Television
CERT	Computer Emergency Response Team
CFAA	Computer Fraud and Abuse Act, 1986
CFIPA	California Financial Information Privacy Act, 2004
CIC	Credit Information Companies
CIDR	Central Identities Data Repository
CJEU	European Union's Court of Justice
Convention 108	The Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data
COPPA	Children's Online Privacy Protection Act, 2000
Cr	Crore
CSP	Cloud Service Providers
CyAT	Cyber Appellate Tribunal
DoT	Department of Telecommunications
DPA	Data Protection Authority
DPB	Data Protection Board
DPDPB 2022	Digital Personal Data Protection Bill, 2022
DPO	Data Protection Officer
EC	European Commission
ECHR	European Convention On Human Rights
ECPA	Electronic Communications Privacy Act,1986
ECtHR	European Court of Human Rights
EEA	European Economic Area
EU	European Union
FCRA	Fair Credit Reporting Act,1970

FedRAMP	Federal Risk and Authorization Management Program
FERPA	The Family and Educational Rights and Privacy Act,1974
FIPPS	Fair Information Practices Principles
FTC	Federal Trade Commission Act, 1994
GB	Gigabyte
GC	Grand Chamber
GDPR	General Data Protection Regulation
GLBA	The Gramm-Leach-Bliley Act,1999
Gmail	Google mail
HEW Committee	Committee in the Department of Health, Education, and Welfare
HIPPA	The Health Insurance Portability and Accountability Act, 1996
ICO	Information Commissioner's Office
IEC	International Electrotechnical Commission
IMC	Indian Medical Council
IMDb	Internet Movie Database
INR	Indian Rupees
IoT	Internet of Things
IPC	Indian Penal Code, 1860
ISO	International Organisation for Standardisation
IT	Information Technology
JPC	Joint Parliamentary Committee
KYC	Know Your Customer
M2M	Machine to Machine
MH	Mental Health
MPSA	Massachusetts Information Privacy and Security Act,2002
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OECD	Organisation for Economic Cooperation and Development
OTT	Over The Top
PC	Personal Computer
PDP 2019	Personal Data Protection Bill, 2019
PFI	Public Financial Institutions
PII	Personally Identifiable Information
RBI	Reserve Bank of India
RTI	Right to Information
SA	Supervisory Authority
SAR	Subject Access Request
SCC	Supreme Court Cases
SCR	Supreme Court Reporter
SME	Small and Medium Sized Enterprise

SMS	Short Messaging Service
SPDI	Security Practices and Sensitive Personal Data or Information
TCPA	Telephone Consumer Protection Act, 1991
TEFU	Treaty Establishing the European Community (renamed the Treaty on the Functioning of the European Union).
TEU	Treaty on European Union
TRAI	Telecom Regulatory Authority of India
TSP	Telecom Service Provider
UCL	Unfair Competition Law
UDHR	Universal Declaration Of Human Rights
UIDAI	Unique Identification Authority of India
UK	United Kingdom
ULA	Unified License Agreement
UN	United Nations
UNCRC	United Nations Convention on the Rights of the Child
US	United States of America
VCDPA	Virginia Consumer Data Protection Act, 2021
VPPA	The Video Privacy Protection Act,1988
WISP	Written Information Security Program

LIST OF CASES

CHAPTER 1 - INTRODUCTION.

Data is all around us and is generated by almost everything we do. The first type of data is the one that we voluntarily share, and the second type is the data that is generated literally every time we do something i.e. whether it's travel, ordering a meal, or using transportation. Without a doubt, this data is extremely valuable, and several companies are willing to pay for access to it. Indeed, in this day and age of universal and nearly free internet access, data is the new currency. What's more intriguing is that the data's full potential is yet unknown.

As technology advances, newer applications emerge, increasing the value of data and also raising several questions, like: to whom does this data belong? Who has access to it? What, if any, restrictions exist on the use of this data? What are the boundaries of privacy? Can data be requested in order to obtain basic services, travel, or even Government benefits? Is national security more important than privacy?

The law, like everything else in technology, is playing catch-up. Jurists all over the world are struggling to reconcile traditional legal concepts with the absurdly intrusive times we live in. This situation is complicated further by the fact that several Governments demand and seek data from their citizens and businesses.

The Supreme Court of India in its landmark judgment on August 24, 2017[2] held that the "*right to privacy*" is a fundamental right guaranteed by Part III of the Indian Constitution. This decision has far-reaching consequences for laws and regulations.

New laws will now be tested using the same criteria that laws that violate personal liberty are tested under Article 21 of the Indian Constitution. The right to privacy is

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

now unambiguously available, and the only remaining question is its contours and limits.

India however currently lacks a comprehensive legislation dealing with data protection and privacy. Existing laws and policies are primarily sectoral in nature. As of now, the relevant provisions are separate from other sectoral legislations.

Apart from other sectoral legislations, the relevant provisions of the Information Technology Act, 2000 and the rules promulgated thereunder currently govern the collection, processing, and use of "*personal information*" and "*sensitive personal data or information*" by a body corporate in India[3] and not by individuals.

2. STATEMENT OF THE PROBLEM:

It has become a business necessity to keep track of people who work with data, as well as the processes used to receive, store, and retrieve data (includes manual and electronic). There are statutory and regulatory requirements to keep these records for a set period of time. This data can be changed, destroyed, tampered with, stolen, repudiated, and so on.

Data can be grouped and labeled as "*non – available*" if it is unavailable at any point during the period of validity. These records were available on a need-to-know basis in manual operations, but in electronic storage, it is simple to make the data unavailable through a variety of options. Distance is no longer a criterion for accessing data, "*access*" is no longer a difficult task since it can break through electronic barriers and yet not break the physical barriers.

[3] Economic Laws Practice, Data Protection & Privacy Issues in India, September 2017, available at : www.elplaw.in (Last accessed on November 12, 2017).

Information Technology has made it easier to access information, efficiently manage difficult processing, evaluate, assess and analyse data for business growth, and contribute to strategy formulation. All of these can be imperiled by a lack of appropriate protection and controls. As a result, regulators have recognised the significance of protecting the privacy of individuals, as well as sensitive data of citizens, in addition to the need for maintaining business records. This has entailed the protection of administrative data in addition to operational or business data.

Organisations have recognised "*Information Technology*" **("IT")** as a crucial component of their operations in order to achieve their objectives. Enterprises used IT for data processing (*e.g*. complex calculators to crunch numbers) about two decades ago, and then transitioned to electronic data processing involving mostly centralised computing. A decade ago, IT has shifted away from *Electronic Data Processing* and began to facilitate *End-User Computing* within an organisation. Its support presently transcends beyond internal end users to partners and customer's mobiles, laptops or desktops, thereby enhancing computing capabilities.

This has increased the challenges of managing ongoing online unwavering support to users, leading to the outsourcing of some internal / external services. Outsourcing has added a new dimension to information access and availability, allowing for more dynamic business decisions at all levels.

This transformation has further resulted in the concept of empowerment at various operational levels, granting employees the authority to make timely, appropriate, and suitable decisions.

The availability aspect of the information system and its technological advancement has opened new avenues to use, misuse and even abuse technology through cheating, fraud and crime. The possibility of empowerment, combined with complexity and exposure to various vulnerabilities, can influence a small percentage

of humans to become inhuman, resulting in dissatisfaction. This can include economic warfare, cyber terrorism and attacks, and so on. Technology has created a slew of new handheld devices, such as: *mobile phones*, *wireless internet access tools*, *remote access tools*, *gadgets*, and so on. As a result, an organisation must consider a systematic approach to controlling their information assets.

With the rapid advancement of technology, computers are now capable of processing massive amounts of data in order to identify correlations and discover patterns in all fields of human activity. Enterprises all over the world have recognised the value of these databases, and the technology for mining and utilising them is evolving on a daily basis and Businesses are developing proprietary algorithms to sift through this data for trends, patterns, and hidden nuances.

The *Internet of Things* **("IoT")** is powered by analogue functions that manage the physical world as they transition to digital functions. It entails incorporating computerization, software, and intelligence into items as diverse as automobiles, toys, aeroplanes, dishwashers, turbines, and dog collars. While not all "things" are connected to the Internet, 20 billion were in 2013, with 35 billion expected in 2022. In 2013, connected "things" accounted for 7% of the total and by 2020, this figure had risen to 15%.[4]

Many of these activities benefit individuals by allowing their problems to be addressed more precisely.[5] Big Data analytics, for example, is used today to analyse very large and complex sets of data. Organisations and Governments can gain remarkable insights into areas such as health, food security, intelligent

[4] The Digital Universe of Opportunities: Rich Data and the Increasing Values of the Internet of Things', EMC Digital Universe with Research and Analysis by IDC, April 2014, available at: https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm, (Last accessed on August 02, 2022).

[5] Roger Parloff, Why Deep Learning is Suddenly Changing your Life', Fortune Magazine (September 28, 2016), available at: http://fortune.com/ai-artificial-intelligence-deep-machine-learning/ (Last accessed on November 10, 2017).

transportation systems, energy efficiency, and urban planning by utilising such analytics.[6] This is comparable to nothing short than a *digital revolution*.

This *digital revolution* has also spread to India. Recognizing its importance and the potential for significant disruption in almost all sectors of society, the Government of India has devised and implemented the "*Digital India*" initiative to empower citizens. This initiative includes the incorporation of digitisation in governance, healthcare and educational services, cashless economy and digital transactions, transparency in bureaucracy, fair and timely distribution of welfare schemes, and so on.

With nearly 450 million Internet users and a 7-8 percent growth rate, India is well on its way to becoming a digital economy with a large market for global players.[7] In the next 40-50 years, this digital economy is expected to create new market growth opportunities and jobs.[8]

The increased use of online platforms such as *Google Pay*, *BHIM*, *Paytm*, *WhatsApp Pay* and numerous other start-ups facilitating digital transactions demonstrates that India has entered an era in which these digital mediums have become an indispensable aspect of our lives, necessitating the establishment of a strong and effective mechanism to provide adequate security to these transactions. With high-speed internet penetration into the country's nooks and corners, the threat to "*informational privacy*" looms larger than ever.[9] While the digitalisation of the economy has created a plethora of job opportunities in sectors such as Healthcare, Education, and Governance, the need for a strong law to ensure maximum

---

[6] European Commission, European Data Protection Reform and Big Data: Factsheet, (2016), available at: http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf (Last accessed on November 08, 2017).

[7] Arushi Chopra, Number of Internet users in India could cross 450 million by June: report, LiveMint , available at: http://www.livemint.com/Industry/QWzIOYEsfQJknXhC (Last accessed on April 02,2017).

[8] Ranjan Guha, Digital Evolution in India, Business Today (August 29, 2017), available at: http://www.businesstoday.in/opinion/columns/digital-evolution-in-india/story/259227.html (Last accessed on December 15, 2017).

[9] Dhiraj R. Duraiswami, Privacy and Data Protection in India, J.L. & Cyber Warfare 166, 169-72 (2017).

protection for individuals' private and personally sensitive data is more important than ever.

To analyse the several causes and its long term effects in the existing scenario, the research study becomes utmost needed and necessary under the present context. The significance of the research study is analysed as under:

3. SIGNIFICANCE OF THE STUDY:

The study becomes relevant owing to the fact that as the number of internet connected devices is increasing, it is likely that a large portion of the data generated by such devices will contain personal and sensitive information about individuals, such as purchases made, places visited, demography, health statistics, financial transactions, education, work profile, and so on.

Electronic Data can now be compressed, sorted, manipulated, discovered, and interpreted like never before, making it easier to transform into useful knowledge[10]. Because of the low costs of storing and processing information, as well as the ease of data collection, long-term storage of information has become common, as has the collection of increasingly minute details about an individual, allowing an extensive user profile to be created.[11]Such data can then be used to create customised user profiles based on their previous online behavior, which has the advantage of shortening the time it takes to complete a transaction. E-commerce websites, for example, track previous purchases and use algorithms to predict what kinds of items a user is likely to buy, reducing the time spent on each purchase.

[10] Helen Nissenbaum, Privacy in Context-Technology, Policy, and the Integrity of Social Life, Stanford University Press, 2010.

[11] Joel Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, Stanford Law Review 1999.

Thus data is fundamentally transforming the way people conduct business, communicate, and make decisions. Enterprises are now compiling massive databases of consumer preferences and behavior to then target such consumers.

Devices (e.g. mobiles, laptops, tablets, and PC's), Telecom Service Providers, and Communication Networks (consisting of switches, routers, and base transceivers), Web Browsers, Operating Systems, Applications, Receiver Stations, *Over the Top* **("OTT")** service providers, *Machine to Machine* **("M2M")** devices, etc, are all part of the Digital Eco-system. The majority of these have gate-keeping capability and an asymmetric advantage of accessing, collecting, and collating data from users, as a result, the users' privacy may be jeopardised. It therefore is critical to ensure that such data is collected, stored, and processed in a controlled manner, and the users' informed and explicit consent is required.[12]

There are numerous advantages of collecting and analysing personal data of individuals, and such pooled datasets enable faster detection of trends and more precise targeting. In the healthcare sector, for example, by collecting and analysing large data sets of individuals' health records and previous hospital visits, health care providers could make diagnostic predictions and treatment recommendations. An individual's personal locational data could be collected and analysed to monitor traffic and improve driving conditions on the road. Banks could use Big Data techniques to improve fraud detection, and insurers could make the process of applying for insurance easier by leveraging valuable knowledge from pooled datasets.[13]

Simultaneously, the Government processes personal data of citizens for a variety of purposes and is arguably the largest processor of personal data. The Government of India, for example, processes personal data for a variety of purposes, including

[12] Report on Privacy, Security and Ownership of the Data in the Telecom Sector, Telecom Regulatory Authority of India , July16, 2018.

[13] Information Commissioner's Office (UK), Big Data, Artificial Intelligence, Machine Learning and Data Protection, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/(Last accessed on November 30, 2017).

targeted delivery of social welfare benefits, effective planning and implementation of Government schemes, counter-terrorism operations, and so on. Such data collection and use is generally regulated by a law, but it appears that this is not the case in the context of counter-terrorism and intelligence gathering.[14]

Thus, as a result, both the public and private sectors are collecting and using personal data on an unprecedented scale and for a variety of purposes. While data can be useful, the unregulated and arbitrary use of data, particularly personal data, has raised concerns about the individual's privacy and autonomy. Some of the concerns revolve around the centralisation of databases, individual profiling, increased surveillance, and the resulting erosion of individual autonomy.

The Researcher through this research attempts to find out where the fault lies, whether the existing laws and legal framework in India is adequate in safeguarding the Digital Privacy of individuals, are there appropriate rules for how personal information should be transmitted, stored, disseminated and distributed online or whether India needs a separate robust legislation for Data Protection.

4. SELECTION OF THE TOPIC WITH REASONING:

The present study titled, *"A COMPARATIVE PERSPECTIVE ON DATA PROTECTION LAWS – WITH REFERENCE TO EUROPE, UNITED STATES OF AMERICA, THE UNITED KINGDOM AND INDIA"*, highlights the necessity to protect personal data as an essential facet of informational privacy while recognising that the protection of personal data holds the key to empowerment, progress, and innovation. Equally implicit is the need to devise a legal framework relating to personal data to protect the autonomy of individuals in relation with their personal data and provide remedies for unauthorised and harmful processing of

[14] Press Information Bureau, Home Minister Proposes Radical Restructuring of Security Architecture, Ministry of Home Affairs, Government of India (December 23, 2009), available at: http://pib.nic.in/newsite/erelease.aspx?relid=56395 (Last accessed on January 06, 2018);

personal data, by adopting learning's from best practices that exist in developed democracies like Europe, United States of America and the United Kingdom with considerably advanced thinking on the subject.

The realm of Confidentiality and Privacy of Personal Data in the digital space has always captivated the Researcher and the inadequacy or near lack of legislation and legal framework to safeguard the same in India further piqued the inquisitiveness of the Researcher and in order to further this interest, the topic under study was selected and researched upon.

After having projected the significance of the study and the reasons for the selection of the topic, the Researcher has also listed down the various objectives that becomes important in the light of the present research study and the reasons as to what it intends to investigate.

5. OBJECTIVES OF THE STUDY:

The present problem under study titled *"A COMPARATIVE PERSPECTIVE ON DATA PROTECTION LAWS – WITH REFERENCE TO EUROPE, UNITED STATES OF AMERICA, THE UNITED KINGDOM AND INDIA"*, has been researched from the socio- legal perspective by the Researcher.

The present research is being carried out keeping the following objectives in mind:

1) To analyse and study the Data Protection Laws in Europe, United States of America, United Kingdom and India.

2) To evaluate and examine the existing legal scenario in India for the personal data protection.

3) To understand the factors that can be incorporated and implemented in framing an independent and robust Data Protection Act, applicable to India.

4) To examine and analyse the adjudication process under the proposed law on matters of privacy in India.

5) To offer suggestions and recommendations that would make the Data Protection Act in India an independent and robust legislation for delivering effective justice against violation of personal data privacy.

A hypothesis establishes the relationship between cause and effect between the issue in question (cause) and what could have induced it (effects), so in order to analyse the said problem in its entirety, the Researcher has highlighted the hypothesis of the present research study under investigation.

6. HYPOTHESIS:

Based on the objectives of the study and the study of review of relevant Literature, the Researcher has formulated the following Hypothesis:

1) The existing laws in India relating to personal data are inadequate and ineffective in protecting the privacy of citizens in the digital space.

2) Lack of an independent and effective Data Protection Law, to address and protect personal data of citizens' leads to violation of Right to Privacy.

3) Other hypothesis of the study is that, there is an impending need for an independent and robust Data Protection Authority that will fulfill and protect the Right to Privacy *vis-a-vis* personal data of citizens' unbiased and without interference of the Government.

4) Present Data Protection legislations in Europe, United States of America and The United Kingdom could be the model basis for protection of data privacy of citizens.

The following is the detailed research methodology that has been adopted by the Researcher in the present study.

7. METHODOLOGY ADOPTED:

The principle of Data Privacy and Data Protection has a wider implication and also a wider interpretation. Thus, the Researcher felt the need to adopt a doctrinal mode of research technique.

In order to understand the concept of data privacy and data protection the Researcher has referred to Primary Resources like Legislations, Judgments, Report of the Committee of Experts under the Chairmanship of Justice B.N.Srikrishna on A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians,2018 **("Justice Srikrishna Committee Report")**, the Personal Data Protection Bill, 2019 **("PDP 2019")**, the Report of the Joint Committee on The Personal Data Protection Bill 2019, 2021 **("JPC Report, 2021")** and the recently proposed Digital Personal Data Protection Bill,2022 **("DPDPB 2022")**, the Government Reports, Report of European Union , the OECD Guidelines, and also the Guidelines of the EU Commission.

The Researcher has also made use of Secondary Resources like the material from the College Library, University and Central Library and the internet sources. The research method adopted for this paper is doctrinal.

8. LIMITATIONS OF THE RESEARCH STUDY

As with the majority of studies, the design of the current study is also subject to limitations. Due to the enormity of the subject, the present study is restricted to comparative analysis of the Data Protection laws of Europe, United States of America and the United Kingdom as they have a robust and considerably advanced legal framework on Data Protection.

The study would focus only in respect of the existing laws applied in India to encompass the issues of Data Protection while not having a separate and independent legislation for the same and is limited to the reports and Bills framed by the legislature in its advent in framing a Data Protection Act for the citizens. The Period of the study is further limited to 5 years. However, the said period may be enhanced in the event of available data is considered inadequate for conducting the study.

9. LITERATURE REVIEW:

The Researcher has examined a variety of literature relating to the principles of ‘Data Protection' and ‘Personal Data Protection’ for the present study.

The Researcher has referred to journals, articles, research papers, and books that provide an in-depth understanding of the best practices of ‘Data Protection’ and ‘Personal Data Protection’ in Europe, United States of America and the United Kingdom and has analysed the existing legal framework, legislations, judgments, committee reports and Bills to trace the evolution of ‘Data Protection' and ‘Personal Data Protection’ in India.

9.1 Commentary, Journals, Articles, Research Papers, and Books on 'Data Protection' and 'Personal Data Protection' prevalent in Europe, United States of America and the United Kingdom :

The European Commission's, Data Protection Working Party Opinion, Opinion 8/2014[15] assesses the growing integration of the Internet of Things **("IoT")** into the lives of European citizens where "smart things" are being made available which monitor and communicate with the homes, cars, work environment and physical activities of individuals in Europe. This Opinion recommends uniform application of the legal data protection framework in the IoT as well as to the development of a high level of protection with regard to the protection of personal data in the EU.

The Handbook on European Data Protection Law[16] summarises the legal standards relating to Data Protection set by the European Union **("EU")** and the Council of Europe **("CoE")** enforced by the EU General Data Protection Regulation, 2018. Since the the data protection reforms carried out by the EU and the CoE are extensive and at times complex, with wide-ranging benefits and impact on individuals and businesses, this handbook raises awareness and improves knowledge of the data protection rules, especially among non-specialist legal practitioners who have to deal with data protection issues in their work. The Handbook also provides for practical illustrations with hypothetical scenarios to illustrate the application of EU General Data Protection Regulation, 2018 in practice.

The Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and The Committee of The

---

[15] European Commission, Data Protection Working Party Opinion, Opinion 8/2014 on the Recent Developments on the Internet of Things, (September 16, 2014), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation /files /2014 /wp223_en.pdf (Last accessed on November 26, 2018).

[16] Handbook on European Data Protection Law, 2018, Information Commissioner's Office (UK), Big Data, Artificial Intelligence, Machine Learning and Data Protection, available at: https://www.echr.coe.int/documents/d/echr/handbook_data_protection_ENG (Last accessed on November 28, 2018).

Regions[17] outlines the comprehensive approach on personal data protection in the European Union. It elaborates the objective of the rules in the current EU data protection instruments to protect the fundamental rights of natural persons and in particular their right to protection of personal data, in line with the EU Charter of Fundamental Right.

The Legal Handbook by Robert Hasty, Dr. Trevor W. Nagel and Mariam Subjally White and Case[18] provides an overview of the US Data Protection Laws as the United States does not have one single data privacy framework or directive it is rather comprised of a patchwork of federal and state laws and regulations, which govern the treatment of data across various industries and business operations. This handbook elucidates the federal statutes in the United States regulate the collection, storage and use of sensitive non-public personal information, and provides the various State legislations, which in contrast, generally regulate the disclosure requirements after a security breach of non-public personal information occurs.

The (UK) Data Protection Act, 2018[19] also known as the UK General Data Protection Regulation is implemented and enforced by the Office of the UK Information Commissioner[20]. The Act provides the guidance and resources on the UKGDPR. The Information Commissioner's Office provides simple and up-to-date information on the data protection and information rights of the members of the Public in the UK including how to make a Subject Access Request, domestic CCTV and data protection, protecting against nuisance marketing and more. It also provides ready guidance to Organisations engaged in direct marketing activities, using cookies or similar technologies, and/or providing electronic communication

[17] The Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and The Committee of The Regions, available at: https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=COM%3A2020%3A324%3AFIN (Last accessed on November 28, 2018).

[18] Robert Hasty, Dr. Trevor W. Nagel and Mariam Subjally White and Case, Data Protection Law in the USA, Advocates For International Development, August 2013, available at: https://www.neighborhoodindicators.org/sites/default/files/course-materials /A4ID_ DataProtectionLaw% 20.pdf (Last accessed on January 08,2019).

[19] Data Protection Act, 2018, available at: https://www.legislation.gov.uk /ukpga/2018 /12/ pdfs /ukpga_ 20180012_ en.pdf (Last accessed on September 28, 2020)

[20] Information Commissioner's Office, available at: https://ico.org.uk/, (Last accessed on September 28, 2019).

services to the public. It details the legal requirements and compliance required to lawfully send electronic marketing messages by phone, email or text, use cookies or similar technologies, or provide electronic communications to the public in the UK and also outlines the what the Organisations need to consider and the actions needed when the Organisation wants to carry out direct marketing activities.

The commentary by Bruce Schneier[21], reasons that while "Anonymous data" sets are an enormous boon for researchers, on the other hand, in the age of surveillance, where everyone collects data on individuals all the time, anonymisation of data is very fragile and riskier than it initially seems as it anonymised data can be used to aggregate a user preference in ways analogous to statistical database queries, which can be further exploited to identify information about a particular user.

The article of Deb Miller Landau[22] evaluates the growing use of Artificial Intelligence **("AI")** in everyday personal life of individuals where its states that an average person generates 600 to 700 megabytes of data per day just doing normal things like posting to Snapchat, sending emails, playing games. The article presents that the more sophisticated the learning becomes, the more data is required for machines to learn which open up possibilities of using neural network models to do things like image recognition and language processing.

The article of Jordi Soria-Comas and Josep Domingo-Ferrer[23], explores the challenges posed by big data in privacy-preserving data management. The article examines the conflicts raised by big data with respect to pre-existing concepts of

---

[21] Bruce Schneier, Why anonymous data sometimes isn't, Wired, December 12, 2017, available at: https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/ (Last accessed on March 03, 2020).

[22] Deb Miller Landau, Artificial Intelligence and Machine Learning: How Computers Learn, IQ Intel, August 17, 2016, available at: https://iq.intel.com/artificial-intelligence-and-machine-learning/ (Last accessed on January 20,2019).

[23] Jordi Soria-Comas and Josep Domingo-Ferrer, Big Data Privacy: Challenges to Privacy Principles and Models, 1(1) Data Science and Engineering, March, 2016, (available at: https://link.springer.com /article /10.1007 /s41019-015-0001-x (Last accessed on January 20, 2019).

private data management, such as consent, purpose limitation, transparency and individual rights of access, rectification and erasure. The article also evaluates how best the two main privacy models used in anonymisation (anonymity and differential privacy) meet the requirements of big data, namely composability, low computational cost and linkability.

The European Commission, authors of articles, handbooks, and the websites, have encapsulated the issues and the legislations prevailing in those respective countries and examined the enforcement of the Data Protection legislations.

The Researcher has in the course of the research become cognisant of the similar research work conducted earlier by research scholars in India, which are highlighted below in order to differentiate these works from the present research being conducted by the researcher:

9.2 Research Papers and Thesis submitted in India:

The Thesis by Ashwini Siwal[24], in 2017, wherein highlights the then prevailing laws related to Data Protection in India, U.S.A. & U.K. However the work has focused primarily on the Inter - Country Problem of Business Process Outsourcing.

The Thesis by Pooja Kiwayat[25], in 2021, has been undertaken to highlight the rationale and jurisprudence behind the data protection laws all over the world with an impetus on the need for affording adequate protection for protecting the informational privacy, highlighting the contours of an effective data protection framework. The thesis analyses various data protection principles that have been developed across the globe while analytically distinguishing the origin of the theme of Data Protection as an aspect of the Right to Privacy and essentially traces the

[24] Ashwini Siwal, available at : http://shodhganga inflibnet.ac.in/hdl.handle.net/10603/307411 (Last accessed on July 25,2022).

[25] Pooja Kiwayat, available at : http://shodhganga inflibnet.ac.in/hdl.handle.net/10603/362372 (Last accessed on July 25,2022).

foundations of the data protection regime while analyzing the several data protection principles recognized by the global institutions all over the world until BREXIT, when the Data Protection Act, 1998 was applicable to the U.K and there was uncertainty on the applicability of EU-GDPR to the U.K. The thesis also undertakes a detailed study of the existing legislations and judicial precedents in the field of right to privacy and data protection within the Indian scheme highlighting a myriad set of lacunas within the Indian data protection framework which is ill equipped to tackle the challenges posed to the informational privacy in the wake of intense digitalisation. It also brings forth the absence of key data protection principles in the existing legislations in the country and further highlights the pressing need to enact a comprehensive data protection code that would recognise the principle of informational self-determination at its helm.

The Thesis by Shivani Joshi[26], in 2019, makes a comparison between the laws relating to data protection in the countries like USA and European Union, and the way data is being protected in India. It considers the laws relating to data protection in the countries like USA and European Union, and the way data is being protected in India. Further it places reliance on the Personal Data Protection Bill 2006 and the Right to Privacy Bill, 2011 in India, which has since become redundant.

The present research on the other hand has considered and analysed the recent developments in the laws related to Data Protection in Europe, United States of America The United Kingdom and India, including the Report of the *Committee of Experts under the Chairmanship of Justice B.N.Srikrishna on A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians,2018* **("Justice Srikrishna Committee Report")**, *the Personal Data Protection Bill, 2019* **("PDP 2019")**, *the Report of the Joint Committee on The Personal Data Protection Bill 2019, 2021* **("JPC Report, 2021")** and the recently proposed *Digital Personal Data*

[26] Shivani Joshi, available at : http://shodhganga inflibnet.ac.in/hdl.handle.net/10603/385428 (Last accessed on July 25, 2022).

Protection Bill,2022 **("DPDPB 2022"),**and focuses on a data protection framework and the architecture for policy on all personal data in India and highlights the areas of concerns therein and suggests a comprehensive data protection framework for India, and as such the present research is different and unique.

10. MODE OF CITATION:

The mode of citation that has been adopted by the Researcher for the purpose of citing footnotes, endnotes, books, researched articles, statutes, rules, ordinances, Journals, magazines, web related search, newspaper articles will be basically on the format adopted in the Blue Book Method of Citation.

The Chapterisation of the thesis is reflected as under:

11. SCHEME OF CHAPTERISATION:

The present research work has been divided/classified into six chapters. A brief summary of each chapter is analysed and is listed herein under:

CHAPTER 1 – INTRODUCTION:

This chapter deals with the introduction of the entire thesis; the Statement of the Problem, Significance of the Study, Selection of the topic with Reasoning, Objectives of the Study, Literature Review, Statement of Hypothesis, Research Methodology adopted, Limitations of the Study and Scheme of Chapterisation.

CHAPTER 2 – PRINCIPLES OF DATA PROTECTION:

In this chapter, the Researcher has focused on the meaning, History and the Need for Data Protection in the present day modern world and has identified the important organisations and the core principles of data protection developed by these organisations and highlighted its need to serve as a reference for nations in developing their own data protection legislation. A number of international and regional organisations have concurred on some of these core principles that must be incorporated into countries' data protection legislation.

CHAPTER 3 – DATA PROTECTION LAWS IN THE EUROPEAN UNION, UNITED STATES OF AMERICA AND THE UNITED KINGDOM:

In this chapter, the Researcher has discussed the legal framework and carried out a comparative analysis of the existing data protection legislations in Europe, United States of America and the United Kingdom in order to understand the best practices adopted on the subject.

CHAPTER 4 – EXISTING DATA PROTECTION LAWS IN INDIA: PRESENT SCENARIO:

In this chapter, the Researcher has enumerated the development in recognition of the Right to Privacy as a Fundamental Right in India through legislative developments and judicial pronouncements, and has studied and examined the present legal framework and the legal provisions contained in various existing laws to secure informational privacy in India**.**

CHAPTER 5 – COMPARATIVE ANALYSIS OF KEY COMPONENTS OF PERSONAL DATA PROTECTION FRAMEWORK :

The Researcher in this chapter, focuses on the key components of personal data as considered by the *Report of the Committee of Experts under the Chairmanship of Justice B.N.Srikrishna on A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians,2018* **("Justice Srikrishna Committee Report")**, *the Personal Data Protection Bill, 2019* **("PDP 2019")**, *the Report of the Joint Committee on The Personal Data Protection Bill 2019, 2021* **("JPC Report, 2021")** and the proposed *Digital Personal Data Protection Bill,2022* **("DPDPB 2022")**, and their ramifications for the impending data protection regulation in India.

CHAPTER 6 – CONCLUSIONS, FINDINGS AND SUGGESTIONS:

In this concluding chapter, the Researcher based on the study seeks to offer conclusions, findings and suggestions derived from the analysis of the best practices of the Data Protection Laws in the European Union, United States Of America and The United Kingdom , attempts to critically analyse the important data protection provision made in the *Report of the Committee of Experts under the Chairmanship of Justice B.N.Srikrishna on A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians,2018* **("Justice Srikrishna Committee Report")**, *the Personal Data Protection Bill, 2019* **("PDP 2019")**, *the Report of the Joint Committee on The Personal Data Protection Bill 2019, 2021* **("JPC Report, 2021")** and the proposed *Digital Personal Data Protection Bill,2022* **("DPDPB 2022")**, while making suggestions to address the shortcomings therein .

The Researcher on the basis of the presentation of information and data has drawn some conclusions and findings applicable to various stakeholders what the study foresees may lead to framing of an independent and robust Data Protection Law in India.

Considering the fact that the Government of India is already in the process of enacting a Data Protection law, no specific suggestion has been made for enacting a new law but the Researcher has attempted to highlight the shortcomings in the proposed draft of the subject law i.e. *the Digital Personal Data Protection Bill, 2022* **("DPDPB 2022")**, and has presented suggestions to address the inadequacy.

CHAPTER 2 : PRINCIPLES OF DATA PROTECTION.

2.1 INTRODUCTION:

Technology, while generally beneficial to humanity does have unintended consequences, for example, increasing use of smart devices in everyday life can lead to a loss of privacy for individuals, who may not even be aware that they are being tracked or observed.

Similarly, the strong presence of smart devices such as a mobile handset has many benefits but can also be a source of user privacy loss, for example, when a user knowingly/unknowingly grants permission to an application to access the camera and micro phone of a smart device; the application can then execute live streaming on the internet using the camera and micro phone, run real time facial recognition algorithms, and use advanced algorithms to create a three dimensional model of the user.

Enterprises all over the world have recognised the value of user data, and as a result, technologies for more accurate data sifting and better understanding of consumer requirements are being developed.[18]

Everyone in today's digital ecosystem has an email address on web-based email platforms. Many users have email accounts on free web-based email platforms, such as Gmail, which offers about 15GB of free storage space for data storage. The emails in the Gmail account typically represent our data, pertaining to our personal or professional matters. Similarly, our expressions of thoughts on Facebook and Instagram and WhatsApp are conveyed in the form of posts, which are also typically data. We are a vital part of the digital and mobile ecosystems in the

[18] 10 Key Marketing Trends for 2017 and Ideas for Exceeding Customer Expectations, IBM, available at: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN (Last accessed on May 07, 2018).

modern era. Its rapid rise over the last two decades has completely altered the way we live our daily lives.

2.2 CONCEPT OF DATA:

The increased computational power of modern computers, combined with the rapid development of technology, has enabled the processing of large amounts of data in order to identify correlations and discover patterns in all fields of human activity, which can even be used for profiling. Individual data can be used to solve problems, ensure targeted delivery of benefits, and bring new products and services to market, among other things.

The Information Technology Act of 2000 as amended by Information Technology (Amendment) Act, 2008 (the "IT Act") describes "Data" as, *"a formalised representation of information, knowledge, facts, concepts, or instructions that is intended to be processed, is being processed, or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the compute*r".[19]

The Government of India's Digital Locker Authority's, Electronic Consent Framework describes "Data" as, *"any electronic information held by a public or private service provider (such as a government service department, a bank, a document repository, etc.), this may include both static documents and transactional documents"*.[20] However, the concept of data extends beyond

[19] Information Technology Act, 2000, Section 2(1)(o) states:- *"Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network. „and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.*

[20] Electronic Consent Framework Technology Specifications, Version 1.1, Section 3.1 states:- *" Data"- Any electronic information that is held by a public or private service provider (like a government service department, a bank, a document repository, etc). This may include both static documents and transactional*

electronic information to include information stored in physical form, such as on a piece of paper. Thus, data collected by such online applications over time may be used for predictive profiling of the individual, putting the user's data privacy at risk.

As the economy increasingly shifts to the digital/online realm, it is critical that users are adequately protected from all entities in the ecosystem that may seek to exploit their gate-keeping power and failure to adequately protect users from the very real risk of harm caused by the loss of privacy may limit the overall growth of the digital economy.

Consequently, not only are we increasingly being reliant on digital data, but with mobile data being generated on a regular basis, everyone is now a global author, publisher, and broadcaster of digital data. Over the last two decades, the volume of such data has also increased drastically.

Whether we have a device or not everything we do generates data in some way or the other. Data is generated by our devices, networks, workplace and even homes. Our transportation systems, automobiles, payment systems, and cities all generate data about and through us. With all of this information, we may be able to make the world a more equitable, better, cleaner, more sustainable, and safer place, however the contrary may also be true.

Our devices and infrastructure are frequently built with data exploitation in mind. This has to change, individuals must have control over their data, including how it is generated, collected, and used. Modern technology's fundamental architecture, functions and operations and deployment must be structured to prevent personal data exploitation.

---

documents, available at https://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework % 20 v1.1.pdf (Last accessed on August 13, 2022).

2.3 DATA PROTECTION AND IMPORTANCE OF PRIVACY:

Data Protection is intended to protect individual's personal information by limiting how such information can be collected, used, and disclosed[21], and because of the emergence of a wide range of issues related to personal information being processed through automated means, it has developed as a legal right in many jurisdictions.

It is thus significant to understand this concept in relation to "*privacy"* because privacy can mean different things depending on the context. There are broadly three types of privacy: *privacy of physical spaces, bodies, and things* **(spatial privacy);** *privacy of certain significant self-defining choices* **(decisional privacy);** and, *privacy of personal information* **(informational privacy)**.[22] Data Protection is primarily associated with the concept of *informational privacy*, but given the pervasiveness of technology, its impact on decisional privacy and spatial privacy is also apparent. Thus, though privacy is commonly associated with seclusion or secrecy, it is understood as a legal right to control over one's personal information.

Privacy is a difficult concept to define because of its complexity, in many cases, the harms caused by violations of privacy are difficult to even identify as they are often intangible. Nevertheless despite its ambiguity, there are a number of reasons why privacy is considered valuable. Individuals can plan and carry out their lives without undue interference when their privacy is protected. Individual's freedom to determine when, how, and to what extent information about them is collected, stored and communicated to others is commonly understood as informational privacy, and it is this autonomy that allows individuals to protect themselves from harm.[23] However, not all information about a person is necessarily private and deserves to be kept private.

---

[21] Lee Bygrave, Data Protection Law: Approaching its Rationale, Logic, and Limits, Kluwer Law International, 2002.
[22] Jerry Kang, Information Privacy in Cyberspace Transactions, Stanford Law Review, April 1998.
[23]Alan F. Westin, Privacy and Freedom, 25 Wash & Lee L. Rev. 166 (1968).

This accordingly gives rise to the "*Data Protection Principles"* which are intended to protect individual's personal information by limiting how such information can be collected, used, and disclosed. Owing to the emergence of a wide range of issues related to personal information being processed through automated means, the Data Protection Principles have become the foundation of legal rights in many jurisdictions.

Certain aspects of an individual's identity are particularly important, such as their bodies, sexuality, or ability to develop their own distinct personalities. Where it legitimately protects an individual's reputation, privacy is also cherished. Even if the information is true, the disclosure of certain inflammatory and sensitive information leads to stereotyping and pre-judging of individuals. In some cases, information about a person (such as race, religion, caste, and so on) can be used to discriminate against them. Some Government actions may also jeopardise an individual's privacy, for example, Government or private surveillance activities on individuals, which can have the alarming effect of disrupting an individual's peace of mind and also create chilling effects by forcing people to conform to a particular societal expectation.

However, as the relevant privacy concerns arise in different contexts, it is not possible to definitively demarcate all of the aspects of privacy requiring protection in this manner. Privacy thus arises not only in a specific, unchanging space such as the home or family, but also in a variety of situations, including public spaces. Different privacy norms can exist in various areas of life, for example, a person may be willing to tell a doctor or psychologist things he or she would never tell his or her spouse or friends.

Thus, to understand these issues, it is necessary to examine how the use of personal information is an important activity in society because it not only reaps many benefits but also has the potential to cause significant harm. Thus, the need for data protection stems from the desire to avoid such harm, and it is hinged on the question

of who should be permitted to use personal information and how,[24]and it is up to a legal framework to decide where such freedom is appropriate and where it is not.

2.4 UNDERSTANDING DATA PRIVACY:

"Data Privacy", also known as *Information Privacy*, is a component of data protection that addresses sensitive data storage, access, retention, immutability, and security.

The proper handling of personal data or *Personally Identifiable Information* **("PII"),** such as names, addresses, social security numbers, and credit and debit card numbers, is typically associated with data privacy. The concept, however, extends to other valuable or confidential data, such as financial information, intellectual property, and personal health information. Industry guidelines, as well as regulatory requirements of various governing bodies and jurisdictions, frequently govern data privacy and data protection initiatives.

Data privacy is therefore, a discipline that includes rules, practices, guidelines, and tools to assist governments and private organisations in establishing and maintaining required levels of privacy compliance.[25]

Data Privacy thus is made up of the six components, which are as follows:

i. **The Legal Framework:** This includes the prevailing legislations, such as the data privacy laws which have been enacted and applied to data privacy related issues.

[24] Pawan Duggal, Data Protection Law in India, Universal Law Publishing, First Edition, 2016.
[25] Stephen J. Bigelow, Data Privacy (Information Privacy), available at: https://www.techtarget.com /searchcio/ definition/data-privacy-information-privacy (Last accessed on August 11, 2017).

ii. **Policies:** These include the established business rules and policies framed to protect the privacy of user's data including employee data.

iii. **Practices:** These comprise the best practices that are established to guide the Information Technology infrastructure in securing data privacy, and data protection.

iv. **Third-Party Affiliations:** These include any third-party organisations that interact with the individual's personal data, such as cloud service providers, etc.

v. **Data Management:** This comprises of the data storage, security, retention, data access standards and practices.

vi. **Global Specifications:** This encompasses the differences in data privacy and compliance requirements between legal jurisdictions around the world.

Data protection and privacy rules must therefore be designed having due consideration to these six components and give individuals the freedom to choose how their personal information is collected, used, and disclosed. This is because it is the individuals who are best equipped to understand how they will benefit or be harmed in the various contexts in which their personal information is used.[26]

Interestingly, though there may be some similarities, data privacy laws are not identical in form to any other existing fields of law such as property, copyright, or tort law, for example, the laws on "defamation" generally prohibit the disclosure of personal information unless it is false. "*Privacy*", on the other hand, would safeguard against the disclosure of accurate personal information.

The origins and applications of privacy thus transcend beyond constitutional law, criminal procedure, and evidentiary rules and defining appropriate regulations for how personal information should be disseminated thus necessitates the use of unique concepts and tools.

[26] http://www.un.org/en/documents/udhr/index.html, (Last accessed on November 20, 2018).

The methods by which we identify harm are an important aspect that emerges in the unique framework of privacy[27] and these can be subjective or objective in nature.

A "*subjective harm"* occurs when an individual has not actually suffered any tangible loss but anticipates such loss following the collection of personal information. The identified harms in this situation are uncertainty, anxiety, and fear of potential scrutiny.

An "*objective harm",* on the other hand, is identified separately when the use of one's personal information actually causes some damage, whether through loss of reputation or some other change in how society treats the individual.

Data protection must thus account for both of these types of harms that result from the unauthorised collection and use of personal information.

2.5 EVOLUTION AND PROGRESSION OF PRIVACY PRINCIPLES:

The use of the *automated data systems* containing personal information about individuals, increased in the 1970s. To address these concerns, the Government of United States of America established an *Advisory Committee in the Department of Health, Education, and Welfare* **("HEW Committee")** to investigate the various legal and technological issues raised by increasingly automated data processing.

The HEW Committee then issued a seminal report titled; *Records, Computers, and Citizens' Rights: Report of the Secretary's Advisory Committee on Automated Personal Data Systems,* in which it recommended that the United States Congress develop a *Code of Fair Information Practices based on Fair Information Practices Principles* **("FIPPS")**. [28]

---

[27] Samuel Warren and Louis Brandeis, The Right to Privacy, Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220.

[28] Pam Dixon, A Brief Introduction to Fair Information Practice Principles, World Privacy Forum (2006), available at: https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/ (Last accessed on December12, 2017).

The FIPPS are a set of principles that govern how data should be handled, stored, and managed in order to maintain fairness, privacy, and security in a rapidly evolving global technological environment.[29] FIPPS are now regarded as the foundation of modern data protection laws all over the world.

In the 1980s, the FIPPS were quickly followed by the *Organisation for Economic Cooperation and Development Privacy Guidelines* **("OECD Guidelines")**.[30] The OECD Guidelines were heavily influenced by the FIPPS and were intended to provide a framework for harmonising national privacy legislations among OECD members while protecting human rights and preventing disruptions in international data flows[31]. The OECD Guidelines are widely regarded as the first internationally agreed-upon statement of core information privacy principles, and they have had a significant impact on individual data protection.

The OECD Guidelines further influenced a number of data protection frameworks, including the *European Directive 95/46/EC on the Processing of Personal data and the Free Movement of such Data* **("Data Protection Directive"),** the *2004 Asia-Pacific Economic Cooperation Framework* **("APEC Framework"),** and data protection legislation, including Australia's *Privacy Act, 1988*, New Zealand's

---

[29] The Fair Information Practices Principles are :

1. There must be no personal-data record-keeping systems whose very existence is secret.

2. There must be a way for an individual, to find out what information about him is in a record and how it is used.

3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.

4. There must be a way for an individual to correct or amend a record of identifiable information about him.

5. Any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

available at https://www.fpc.gov/resources/fipps/ (Last accessed on March 30,2018).

[30] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), available at:http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Last accessed on February 07, 2018).

[31] Sian Rudgard, A Race for Maintaining Personal Data - How to Manage Consumers' data under the Right to Be Forgotten and the Right to Data Portability of the new EU GDPR, available at https://run.unl.pt/bitstream/10362/38767/1/Vale_2018.pdf (Last accessed on January 05,2019).

P*rivacy Act, 1993*, and Japan's *Protection of Personal Information Act, 2003*.[32] Nonetheless, despite its popularity, these traditional privacy principles have come under considerable scrutiny in recent times, as it has been argued, it may not be well-suited to address the challenges posed by the dramatic increase in the volume and use of personal data, advances in computing, and global data flows.

The challenges posed included, privacy management programmes to improve data controller accountability, data security breach notifications, which required data controllers to notify individuals/authorities of a security breach, and the establishment and upkeep of privacy enforcement authority.[33] More cross-border data flows and international co-operation to improve global interoperability of privacy frameworks were also identified as critical components of a global data economy.

The OECD Guidelines have also been criticised as being fundamentally incompatible with modern technologies and Big Data analytics, which have revolutionised data collection and processing.[34]

Corporations now have data that has been generated or collected from a wide range of sources. Financial data, employee data, and customer data are examples of such data.

Big Data is typically defined by three V's, i.e.: *volume* (as in massive datasets), *velocity* (as in real-time data), and *variety* (as in different data sources).

Other technological advancements, such as *Artificial Intelligence* **("AI")**[35], *Machine Learning*[36], and the *Internet of Things* **("IoT")**[37], are all part of the Big Data

[32] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), available at:http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Last accessed on January 07, 2019).

[33] Organisation for Economic Co-operation and Development, Thirty Years After: The OECD Privacy Guidelines (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (Last accessed 05 January 2019).

[34] *Supra* note 23.

ecosystem and are becoming more widely used. Given these developments, the most difficult challenge in regulating such emerging technologies is that they may operate outside of the framework of traditional privacy principles.

The introduction of these technologies has also broadened the realm of personal data. Big Data has radically expanded the range of personally identifiable data, for example, by analysing meta-data such as a set of predictive or aggregated findings or by combining previously discrete sets of data, non-personal information data can now be combined with other data sets to create personally identifiable information.
A further example of this is how anonymised Netflix data on film rankings could be easily combined with other data sets such as timestamps and public information from the *Internet Movie Database* **("IMDb")** website to de-anonymise the original data set and reveal individual personal movie preferences.[38]

Similarly, Big Data relies on the accumulation of large volumes of data to extract information from them, making data minimisation difficult to apply. Furthermore, technologies like the IoT rely on the continuous collection of personal information from smart device users, which can then be interpreted to provide unique services.[39]

As a result, adhering to the traditional privacy principles of consent, collection, and use limitation may be difficult in such cases and given the rapid development of

---

[35] The Society for the Study of Artificial Intelligence and Simulation of Behaviour, What is Artificial Intelligence, available at: http://www.aisb.org.uk/public-engagement/what-is-ai (Last accessed on February 19, 2019).

[36] Machine Learning is defined as the set of techniques that allow computers to think by creating mathematical algorithms based on accumulated data. See also Deb Miller Landau, Artificial Intelligence and Machine Learning: How Computers Learn, IQ Intel (17 August 2016), available at: https://iq.intel.com/artificial-intelligence-and-machine-learning/ (Last accessed on February 19,2019).

[37] Data Protection Working Party Opinion, Opinion 8/2014 on the Recent Developments on the Internet of Things, European Commission (16 September 2014), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf,(Last accessed on February 19, 2019).

[38] *Supra* note 21.

[39] *Supra* note 34.

these emerging technologies, alternatives to traditional privacy principles have been proposed, which require careful consideration.[40]

Technologies like *Big Data*, the *IoT*, and *AI* are here to stay and hold the promise of welfare and innovation, India will therefore need to develop a data protection law that can successfully address the issues associated with such emerging technologies in order to strike a balance between innovation and privacy. It will be necessary to carefully determine whether this involves a reiteration of traditional privacy principles, an alternative approach based on newer ex-ante forms of regulation, or a hybrid model.

The Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, both of which India is a signatory, show that the right to privacy is recognised internationally. The *Universal Declaration of Human Rights* (also known as the *Human Rights Declaration or* **"UDHR"**), adopted by the United Nations General Assembly on December 10, 1948 was the obvious starting point for establishing standards for individual protection.

The Human Rights Declaration recognised what are now universal values and traditions, recognising, the inherent dignity and equal and inalienable rights of all members of the human race as the foundation of global freedom, justice, and peace.[41] The Human Rights Declaration includes specific provisions relating to the right to a private and family life, as well as the right to free expression without regard to borders. In fact, the Human Rights Declaration's principles have served as the foundation for all subsequent European data protection laws and standards.

---

[40] *Ibid* at 39.

[41] Universal Declaration of Human Rights, Preamble, available at https://www.un.org/en/about-us/universal-declaration-of-human-rights (Last accessed on March 15, 2020).

While Article 12 of the Human Rights Declaration contains the right to a private life and associated freedoms[42], Article 19 of the said Human Rights Declaration contains the right to freedom of expression.[43] Though the provisions of Article 19 may appear to contradict the provisions of Article 12, particularly where their application may result in an invasion of privacy in violation of Article 12. It is Article 29(2) of the Human Rights Declaration that reconciles this apparent contradiction by stating that individual rights are not absolute and that a balance must be struck to limit their exercise.[44]

Furthermore, Article 17(1) of the *International Covenant on Civil and Political Rights*, to which India is also a signatory, protects individuals from arbitrary or unlawful interference with their privacy, family, home, and correspondence, as well as unlawful attacks on their honour and reputation.[45]

Article 8 of the *European Convention on Human Rights* **("ECHR")**, provides for the right to respect for private and family life, and Article 8(1) expressly provides for, the right to respect for an individual's private and family life, his home, and his correspondence.[46]

Furthermore, Article 8(2) of the said ECHR prohibits interference by a public authority except such as may be necessary in a democratic society in the interest of

---

[42] Universal Declaration of Human Rights, 1948 , Article 12 states :- *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

[43] Universal Declaration of Human Rights, 1948, Article 19 states :- *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*

[44] Universal Declaration of Human Rights, 1948, Article 29 states:- - *In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.*

[45] International Covenant on Civil and Political Rights, Article 17 states:-
1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

[46] Convention for the Protection of Human Rights and Fundamental Freedoms, 1950, Article 8(1) states:-
Freedoms - Everyone has the right to respect for his private and family life, his home and his correspondence.

national security, public safety, or the economic well-being of the country, for the protection of health or morals, or for the protection of others' rights and freedoms.[47]

Thus, data protection is commonly considered as the law that is intended to protect an individual's personal information that is collected, processed, and stored using "automated" means or that is intended to be part of a filing system.

Data protection laws in modern societies must restrain and shape the activities of businesses and governments in order to empower the individuals to control their information and protect them from abuse, as these institutions have repeatedly demonstrated that unless rules limit their actions, they will attempt to collect, mine, and keep everything while disclosing nothing. As a result, as citizens and consumers, individuals must have a way to exercise their right to privacy and protect themselves and their information from misuse and abuse. This is particularly true when it comes to personal information. Data protection is concerned with the safeguarding of the individual's fundamental right to privacy, which is enshrined in international and regional laws and treaties.

Businesses and Governments have been storing personal information of individuals in databases since the 1960s, as information technology has advanced databases can now be searched, edited, and cross-referenced, and data can be shared with organisations and individuals worldwide. As a result of all of this, as well as growing public concern, the data protection principles were developed through numerous national and international consultations.

The first law was passed in the German State of Hesse in 1970, and the 1970 *Fair Credit Reporting Act* in the United States of America included some data protection provisions. The United States led the development of *"fair information practices"* in

---

[47] Convention for the Protection of Human Rights and Fundamental Freedoms, 1950, Article 8(2) states:-- *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

the early 1970s, which continue to shape data protection law even today. Around the same time, the United Kingdom also formed a committee to investigate private sector threats and reached similar conclusions.

National laws soon followed, beginning with Sweden, the United States, Germany, and France. The OECD added to the momentum in 1980 when it issued privacy guidelines that included "privacy principles"[48], and the Council of Europe's convention entered into force shortly after.

2.6 RATIONALE FOR DATA PROTECTION:

The use of computers to process information about individuals which increased in the early 1970s coincided with the development of the *European Economic Community*, which resulted in an increase in cross-border trade and, as a result, more sharing of personal information was made possible.

Rapid advances in electronic data processing, as well as the introduction of mainframe computers, further enabled public administrations and large corporations to establish extensive data banks and improve the collection, processing, and sharing of personal information.[49] Additionally, computers in combination with the advancement of telecommunications, created new opportunities for international data processing.

Although these developments provided significant benefits in terms of efficiency and productivity, they also raised concerns that these otherwise positive advancements would have a negative impact on individuals' privacy, which would

[48] Bhumesh Verma and Ujjwal Agrawal, Evolution of Data Privacy, Sayantan Dey Legal and Compliance Professional, available at: https://www.scconline.com/blog/post/2020/02/06/evolution-of-data-rivacy/#:~:text=Privacy%20was%20statutorily%20recognised%20globally,provisions%20in%20their%20domestic%20laws, (Last accessed on August 25, 2022).

[49] Sian Rudgard, Origins and Historical Context of Data Protection Law, available at; https://www.scribd.com/document/435237603/European-Privacy-Chapter-One (Last accessed on August 05, 2019).

be exacerbated when personal information was transferred across international borders.

Individual state legal systems in Europe already had some rules aimed at protecting individuals' personal information, such as laws on privacy, tort, secrecy, and confidentiality. However, it was recognised that the automated storage of personal information, as well as the rise in cross-border trade, necessitated the development of new standards that allowed individuals to retain control over their personal information while allowing the free international flow of information required to support international trade.

The challenge was to frame these standards in a way that maintains a balance between national concerns about personal freedom and privacy and at the same time support for free trade.

2.6.1 Universal Declaration Of Human Rights (“UDHR”):

The obvious starting point for developing standards for individual protection was the *Universal Declaration of Human Rights* (also known as the *Human Rights Declaration*), which was adopted by the United Nations General Assembly on December 10, 1948.

The UDHR recognised what are now regarded as the universal values and traditions, recognising, the inherent dignity and equal and inalienable rights of all members of the human race as the foundation of freedom, justice, and peace in the world.

The UDHR includes specific provisions regarding the right to a private and family life, as well as the right to free expression regardless of borders. In fact, the principles enshrined in the UDHR served as the foundation for all subsequent European data protection laws and standards.

The right to a private life and related freedoms enshrined in Article 12 and 19 of the UDHR[50] and the right to free expression[51] came to be considered as the fundamental aspect of the UDHR.

2.6.2 European Convention On Human Rights ("ECHR"):

The Council of Europe invited individual states to sign the *European Convention on Human Rights* **("ECHR")**, an international treaty designed to protect human rights and fundamental freedoms, in Rome in 1950. It went into effect on September 3, 1953, and was based on the Human Rights Declaration. Since the ECHR only applies to member states, it is referred to as a "*closed instrument".*

All the Council of Europe member states have ratified the ECHR, and new members are expected to do so as soon as possible. Parties to the ECHR commit to guaranteeing these rights and liberties to everyone within their jurisdiction.

Owing to the wide span of the fundamental rights and liberties of individuals it protects, the ECHR is considered to be a very potent tool. These include *the right to life, the prohibition of torture, the prohibition of slavery and forced labour, the right to liberty and security, the right to a fair trial, the prohibition of punishment without a trial, the respect for private and family life, the freedom of thought, conscience, and religion, the freedom of expression, the freedom of assembly and association, the right to marry, the right to an effective remedy,* and *the prohibition of discrimination.*

The ECHR is also significant because it established a system of enforcement in the form of the *European Court of Human Rights* **("ECtHR")**, which investigates alleged ECHR violations and ensures that member States comply with their ECHR

[50] *Supra* note 42.
[51] *Supra* note 43.

obligations. Decisions of the ECtHR are binding on the member States involved and can result in legislation or practice changes by the respective national governments. The ECtHR may also issue advisory opinions on the interpretation of the ECHR and the protocols at the request of the Council of Europe's Committee of Ministers.

It is pertinent to note that Article 8 of the ECHR[52] is a paraphrase of Article 12 of the UDHR, and both recognise the need for a balance between individual rights and justifiable interference with those rights, which is a recurring theme in data protection law.

The fundamental rights and liberties of individuals established in the UDHR and the ECHR thus laid down the rationale for the data protection.

2.7 EARLY LAWS AND REGULATIONS IN EUROPE ON USE OF PERSONAL INFORMATION:

From the late 1960s to the 1980s, a number of countries, mostly in Europe, led the way in enacting legislation aimed at limiting Government agencies and large corporation’s use of individual’s personal information and countries like Austria, Denmark, France, the Federal Republic of Germany, Luxembourg, Norway, and Sweden led the way, with legislations protecting individual information protection, *albeit* in a limited way.

Data protection has also been enshrined as a fundamental right in the constitutions of three European countries, i.e. Spain, Portugal, and Austria. In light of this trend, the Council of Europe decided to create a framework of specific principles and standards to prevent unfair data collection and processing in Europe. This was in response to concerns that, in the context of emerging technology, the national legislation did not adequately protect the ECHR's Article 8 right of respect for the

[52] *Supra* note 46.

individual's private and family life, his home, and his correspondence. This concern prompted the release of *Recommendation 509 on Human Rights and Modern and Scientific Technological Developments* in 1968.[53]

The Council of Europe further expanded on this preliminary work in 1973 and 1974 with *Resolutions 73/22* and *74/29*, which established principles for the protection of personal data in automated databanks in the private and public sectors respectively, with the goal of setting in motion the development of national legislation based on these resolutions.

This was deemed as an urgent requirement due to concerns that there was already divergence between the member States laws in this area. It became clear that comprehensive protection of personal information could only be achieved by further reinforcing such national rules through binding international standards.

---

[53] Council of Europe, Recommendation 509 on Human Rights and Modern and Scientific Technological Developments in 1968 states:- *The Assembly,*

(1) Considering that member States under the Statute of the Council of Europe accept the principle of the enjoyment by all persons within their jurisdiction of human rights and fundamental freedoms;

(2) Having regard to the serious dangers for the rights of the individual inherent in certain aspects of modern scientific and technological development;

(3) Believing that newly developed techniques such as phone-tapping, eavesdropping, surreptitious observation, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda are a threat to the rights and freedoms of individuals and, in particular, to the right to privacy which is protected by Article 8 of the European Convention on Human Rights;

(4) Considering that the law in the majority of the member States does not provide adequate protection against such threats to the right of privacy, and that there is in consequence danger of violation of Article 8 of the Convention on Human Rights;

(5) Noting that some member States of the Council of Europe are planning to revise their legislation on this subject and that it would be desirable for any such reform to tend towards a greater harmonisation of the law ;

(6) Considering that it would be useful to make a detailed study of the legal problems arising in connection with the right to privacy and its violation by modern technical devices, with special reference to the European Convention on Human Rights;

(7) Reserving the right to continue its own studies and to make further proposals on the questions concerned,

(8) Recommends that the Committee of Ministers instruct the Committee of Experts on Human Rights :

8.1. to study and report on the question whether, having regard to Article 8 of the Convention on Human Rights, the national legislation in the member States adequately protects the right to privacy against violations which may be committed by the use of modern scientific and technical methods;

8.2 if the answer to this question is in the negative, to make recommendations for the better protection of the right of privacy.

available at : https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en, (Last accessed on July 18, 2020).

Other significant initiatives in the early 1980s came from the OECD and the Council of Europe in the form of the *OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*[54] and the Council of Europe *Convention for the Protection of Individuals Regarding Automatic Processing of Personal Data*.[55]

2.7.1 Organisation For Economic Co-Operation And Development ("OECD") Guidelines:

Broadly speaking, the OECD's role was to promote policies aimed at achieving the highest sustainable economic growth, employment, and rising living standards in both OECD member and non-member countries, while maintaining financial stability and thus contributing to the global economy's development.

Interestingly, the OECD membership includes a number of countries outside of Europe.

In order to facilitate the harmonisation of data protection law between the member countries, the OECD developed *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* **("OECD Guidelines")** in 1980[56], laying down basic rules governing trans-border data flows and the protection of personal information and privacy.

These OECD Guidelines were published on September 23, 1980, in close collaboration with the Council of Europe and the European Community. Though these are not legally binding, they are intended to be flexible and aimed to serve as a foundation for legislation in member countries where there is no data protection

[54] *Supra* note 30.
[55] Council of Europe Convention for the Protection of Individuals Regarding Automatic Processing of Personal Data, available at: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.(Last accessed on June 20, 2021).
[56] *Supra* note 30.

legislation, or serve as a set of principles that can be incorporated into existing data protection legislation.

As the OECD's membership extends beyond Europe, the OECD Guidelines have a broad impact. The emphasis is on collaboration with other countries in order to avoid gaps in the implementation of these guidelines among OECD member countries.

In subsequent declarations issued in 1985 and 1998, the OECD reaffirmed its commitment to the OECD Guidelines.

The OECD made every effort to ensure consistency with the principles being developed on behalf of the Council of Europe, which means that there are clear parallels between the OECD Guidelines and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Further, the OECD Guidelines aim to strike a balance between protecting individuals' privacy and rights and freedoms while not impeding trade and allowing the free flow of personal data across national borders.

The OECD Guidelines interestingly make no distinction between public and private sectors. Importantly, they are agnostic to the technology used, making no distinction between automated and non-automated personal information. Though it acknowledges that some processing involves both automated and non-automated systems, and that focusing solely on computers may lead to inconsistency as well as may provide opportunities for data controllers to circumvent national laws that implement the OECD Guidelines by processing personal information in non-automatic ways. The focus of the OECD Guidelines was to thus to protect personal information, the processing of which could *'endanger privacy and individual liberties*'.

The OECD Guidelines recommended certain principles of data protection to apply for personal data, whether in the public or private sectors, that pose a risk to privacy and individual liberties due to the way they are processed, their nature, or the context in which they are used. The Principles recommended by the OECD Guidelines are as follows:

i. **Principle of Collection Limitation**[57] : This Principle states that the personal data collection should be limited, and any such data should be obtained lawfully and fairly, and, where appropriate, with the knowledge or consent of the data subject i.e. the individual.
ii. **Principle of Data Quality**[58] : This Principle provides that the personal data collected should be relevant to the purposes for which it is to be used, and should be accurate, complete, and up to date to the extent necessary for those purposes.
iii. **Principle of Purpose Specification**[59] : This Principle requires that the purpose(s) for which personal data are collected should be specified as soon as possible after data collection, and its subsequent use should be limited to the fulfillment of those purposes or such others that are not incompatible with those purposes and are specified on each occasion of change of purpose.
iv. **Limitation of Use Principle**[60] : This Principle requires that the personal data collected should not be disclosed, made available, or otherwise used for purposes other than those specified in the purpose for which the data is collected unless:

---

[57] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data **,** Collection Limitation Principle states:-- *There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.*

[58] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**,** Data Quality Principle states:- *Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.*

[59] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data **,** Purpose Specification Principle states:- *The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.*

[60] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data **,** Use Limitation Principle states:- *Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:*
a) with the consent of the data subject; or
b) by the authority of law.

a) the data subject consents; or

b) the authority of law requires it.

v. **Principle of Security Safeguards**[61] : This Principle states that the personal data collected should be safeguarded by reasonable security measures against risks such as data loss or unauthorised access, destruction, use, modification, or disclosure.

vi. **Principle of Openness**[62] : This Principle states that there should be a general policy of transparency regarding personal data developments, practices, and policies. It further provides that there should be easy ways to establish the existence and nature of personal data, as well as the primary purposes, for which they are used, as well as the identity and usual residence of the data controller.

vii. **Principle of Individual Participation**[63] : In terms of this Principle, an individual should have the right to:

a) obtain confirmation from a data controller, or otherwise, of whether or not the data controller has data relating to him;

b) have data relating to him communicated to him within a reasonable time, at a reasonable charge, in a reasonable manner and in a form that is readily understandable.

---

[61] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data **,** Security Safeguards Principle states:- *Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.*

[62] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data **,** Openness Principle states: - *There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller*.

[63] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data **,** Individual Participation Principle states:- *An individual should have the right:*
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

c) to be informed of the reasons if a request made is denied, and to be able to dispute such denial, and;

d) to challenge data relating to him, and to have the data erased, rectified, completed, or amended if the challenge is successful.

viii. Principle of Accountability[64] **:** In terms of this Principle, a data controller should be held accountable for implementing measures that give effect to the aforementioned principles.

Nevertheless, despite their popularity, these traditional privacy principles have come under considerable scrutiny in recent times.

2.7.2 The Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data ("Convention 108"):

On January 28, 1981 the Council of Europe adopted the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* **("Convention 108")** and made it available for signature to the Council of Europe member States. The fact that it was not referred to as the European Convention indicated that it was open to countries outside of Europe to join.

Convention 108 was the first legally binding international instrument in the field of data protection. It differs from the OECD Guidelines as in that being legally binding it required signatories to implement the principles it establishes in their domestic legislation in order to ensure respect for the fundamental human rights of all individuals in the processing of personal information. The Council of Europe stated in Convention 108 that those who hold and use personal information in computerised form have a social responsibility to protect such personal information,

---

[64] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data **,** Accountability Principle states :- *A data controller should be accountable for complying with measures which give effect to the principles stated above.*

especially since decisions affecting individuals are increasingly based on information stored in computerised data files.

The preamble to this Convention 108 provided that its goal is to achieve greater unity among its members and to expand safeguards for everyone's rights and fundamental freedoms, particularly the right to privacy, in light of the increasing cross-border transfer of personal data undergoing automated processing.[65]

Thus, Convention 108 is the first legally binding international instrument to establish standards for the protection of individual's personal data while also attempting to strike a balance between those safeguards and the need to maintain the free flow of personal data for the purposes of international trade.

2.7.3 The Treaty of Lisbon ("Lisbon Treaty"):

The Treaty of Lisbon **("Lisbon Treaty")** was signed on December 13, 2007, and came into effect on December 1, 2009. Its primary goal is to strengthen and improve the European Union's **("EU")** core structures so that it can function more efficiently.[66] The Lisbon Treaty modifies the EU's two foundational treaties i.e. *the Treaty on European Union* and the *Treaty Establishing the European Communit*y (renamed the *Treaty on the Functioning of the European Union,* or **"TFEU"**).

Article 16(2)[67] of the TFEU requires all European Union institutions to protect individuals when processing personal data. It provided for a designated European

---

[65] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,1981, available at : https://rm.coe.int/1680078b37 (Last accessed on June 24,2021).

[66] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, available at: http://europa.eu/lisbon_treaty/index_en.htm. (Last accessed on July 25, 2020).

[67] Treaty on the Functioning of the European Union, Article 16 (2) (ex Article 286 TEC) states:- *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*
available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF (Last

Data Protection Supervisor whose role it is to ensure compliance with data protection law within the European Union institutions, and it implies that national data protection authorities may also have jurisdiction in such matters. One of the main goals of the Lisbon Treaty is to promote a number of core values such as, human dignity, freedom, democracy, equality, the rule of law, and respect for human rights. These values are shared by all member countries, and any European country seeking to join the European Union must uphold them.

This is a significant development because the European Union's earlier treaties made no mention of fundamental rights. The Lisbon Treaty prioritises the areas of justice, freedom, and security, and a significant change in this area is the introduction of a single common legal framework for all EU activities, consisting of a single system through which the EU can govern on matters of data protection.

2.7.4 The 1995 Data Protection Directive 95/46/EC of the European Union :

In 1995, the European Union attempted to address some of the issues raised by the OECD framework's mosaic of European privacy laws. To accomplish this, the *European Commission* **("EC")** issued a new "directive" that was now binding on all EU member states in the form of *The Data Protection Directive 95/46/EC*[68] which required each EU member state to adopt privacy laws that are *"equivalent"* to one another. It also stated that data could only be exported to third-party countries that could provide *"an adequate level of protection"* for European citizens' data via domestic laws or international commitments.

---

accessed on July 25, 2020)

[68] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 On The Protection Of Individuals With Regard To The Processing Of Personal Data and on The Free Movement Of Such Data, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 (Last accessed on June 28,2020).

2.7.5 Charter of Fundamental Rights of the European Union ("Charter") :

Recognising that its policies could have an impact on human rights and seeking to bring citizens closer to the EU, the EU proclaimed the *Charter of Fundamental Rights of the European Union* in 2000 **("Charter")**[69]. By combining constitutional traditions and international obligations shared by the member States, it incorporates the full range of civil, political, economic, and social rights of European citizens.

The Charter's rights are divided into six categories viz: *dignity*, *freedom*, *equality*, *solidarity*, *citizen's rights*, and *justice*.

Initially only a political document, the Charter became legally binding as EU primary law on December 1, 2009, when the Lisbon Treaty entered into force. The provisions of the Charter are addressed to EU institutions and bodies, requiring them to respect the rights listed in the Charter while carrying out their responsibilities. The provisions of the Charter bind member States when they implement EU law.

The Charter not only guarantees respect for private and family life (Article 7)[70], but it also establishes the right to personal data protection (Article 8).[71] The Charter also expressly elevates this level of protection to that of a fundamental right under EU law. This right must be guaranteed and respected by EU institutions and bodies, as well as by Member States when implementing Union law.[72] Further, the Charter

---

[69] Charter Of Fundamental Rights Of The European Union (2000/C 364/01), available at : https://www.europarl.europa.eu/charter/pdf/text_en.pdf (Last accessed on June 28,2020).

[70] Charter Of Fundamental Rights Of The European Union, Article 7 states: - *Respect for private and family life Everyone has the right to respect for his or her private and family life, home and communications.*

[71] Charter Of Fundamental Rights Of The European Union, Article 8 states: - *Protection of personal data :*
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

[72] Charter Of Fundamental Rights Of The European Union, Article 51states: - *Scope*
1. The provisions of this Charter are addressed to the institutions and bodies of the Union with due

mandates the establishment of an independent authority to oversee the implementation of the data protection principles.

The Charter provides that the right to personal data protection is not an absolute right, it can be limited if it is necessary to achieve a general goal or to protect the rights and freedoms of others.

Article 8 of the ECHR and Article 52 (1) of the Charter specify the conditions for limiting the rights to respect for private life and personal data protection. They have been developed and interpreted through case law of the European Court of Human Rights ("ECtHR").

2.7.6 The European Court of Human Rights ("ECtHR") :

The ECtHR has treated the concept of "private life" as a broad concept in its judgments, including aspects of professional life and public behaviour. It has also ruled that the protection of personal data is an important component of the right to privacy. Nonetheless, despite the broad interpretation of private life, not all types of processing would necessarily jeopardise the rights guaranteed by Article 8 of the ECHR.

The ECtHR vide its judgments has consistently held that an interference is legal only if it is based on a provision of domestic law that meets certain criteria. The law must be accessible to the persons concerned and predictable in terms of its consequences. The relevant judgments of the ECtHR are as under:

---

2. *regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers.*
3. *This Charter does not establish any new power or task for the Community or the Union, or modify powers and tasks defined by the Treaties.*

i. In ***Rotaru v. Romania***[73], the applicant alleged a violation of his right to privacy as a result of the Romanian Intelligence Service's possession and use of a file containing his personal information. The ECtHR determined that, while domestic law permitted the gathering, recording, and archiving of information affecting national security in secret files, it did not impose any limitations on the exercise of those powers, which remained at the discretion of the authorities. Domestic law, for example, did not specify the type of information that could be processed, the types of people against whom surveillance measures could be used, the circumstances under which such measures could be used, or the procedure to be followed. As a result, the Court concluded that the domestic law failed to meet the requirement of foreseeability under Article 8 of the ECHR, and that this article had been violated.

ii. The applicant in ***Taylor-Sabori v. the United Kingdom***[74], had been the subject of police surveillance. The police intercepted messages sent to the applicant using a 'clone' of his pager. The applicant was detained and charged with conspiracy to distribute a controlled substance. The contemporaneous written notes of the pager messages, which the police had transcribed, formed part of the prosecution's case against him. However, there was no provision in British law governing the interception of communications transmitted via a private telecommunications system at the time of the applicant's trial. As a result, the violation of his rights was not "in accordance with the law." The ECtHR determined that this was a violation of Article 8 of the ECHR.

iii. In ***Peck v. the United Kingdom***[75], the applicant attempted suicide on the street by cutting his wrists while unaware that he was being watched by a CCTV

---

[73] Rotaru v. Romania, [ECtHR GC] No. 28341/95, available at : https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]} (Last accessed on August 17, 2020).

[74] Taylor-Sabori v. the United Kingdom, ECtHR No. 47114/99, available at http://hudoc.echr.coe.int › app › conversion › docx (Last accessed on August 17, 2020).

[75] Peck v. the United Kingdom, ECtHR No. 44647/98, available at : https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22003-687182-694690%22]} (Last accessed on August 17, 2020).

camera. The police, who were watching the CCTV cameras, rescued him and later gave the CCTV footage to the media, who published it without masking the applicant's face. The ECtHR determined that there were no relevant or sufficient reasons to justify the authority's direct disclosure of the footage to the public without first obtaining the applicant's consent or masking his identity. The Court concluded that Article 8 of the ECHR had been violated.

Thus, it can be inferred from the judgments of the ECtHR mentioned above, that the EC recognised a small number of third-party countries as having an "adequate" legal framework for protecting the data of EU citizens. The nations of Andorra, Argentina, Canada, the Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay were among those countries. As a result, these countries could transfer EU citizens' data without further authorisation.

Notably, the EC did not consider the protections provided by US law to be "adequate".

2.8 FOUNDATION OF DATA PROTECTION PRINCIPLES IN THE UNITED STATES OF AMERICA:

Although the right to privacy was a long-established fundamental right in international legal order, the United Nations framework did not recognise personal data protection as a fundamental right. Article 12[76] of the UDHR on respect for private and family life established an individual's right to privacy from others, particularly the state, for the first time in an international instrument. Despite being a non-binding declaration, the UDHR has significant status as the foundational instrument of international human rights law, and has influenced the development of other human rights instruments in America.

[76] Supra note 69.

2.8.1 The Safe Harbor Framework:

The European Commission approved a **"Safe Harbor Framework"** developed by the U.S. Department of Commerce on July 26, 2000.[77] This framework established a set of fair data information practices that participants agreed to follow. To comply with the requirements of the framework, the participants agreed to increased enforcement and oversight by two U.S. regulatory agencies i.e. the *Federal Trade Commission* **("FTC")** and the *Department of Transportation* .

The Safe Harbor Framework laid down seven principles regarding data protection, which are as follows:

i. **Principle of Notice**[78]**:** This Principle provides that the individuals must be informed about the purposes for which organisations collect and use information about them.
ii. **Principle of Choice**[79] **:** This Principle states that the organisations must allow individuals to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the original or later authorised purpose for which it was collected.
iii. **Principle of Onward Transfer (Transfer to Third Parties)**[80] **:** This Principle provides that organisations must follow the notice and choice principles when disclosing information to a third party[81].

---

[77] Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks, available at: https://www.ftc.gov/business-guidance/resources/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor-frameworks (Last accessed on August 23, 2020).

[78] US-EU Safe Harbor Framework Principle, Notice states:- -*Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure*.

[79] US-EU Safe Harbor Framework Principle , Choice states: - *Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or later authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.*

[80] US-EU Safe Harbor Framework Principle, Onward Transfer (Transfer to Third Parties) states: - *To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the Safe Harbor Privacy Principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written*

iv. **Principle of Access**[82] **:** This Principle provides that individuals must have access to personal information about themselves that an organisation holds and must be able to correct, amend, or delete that information if it is inaccurate, unless the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case at hand, or if the rights of persons are violated.

v. **Principle of Security**[83]**:** This Principle requires that the organisations must take reasonable steps to safeguard personal information against loss, misuse, and unauthorised access, disclosure, alteration, and destruction.

vi. **Principle of Data Integrity**[84] **:** This Principle provides that personal information must be pertinent to the purposes for which it will be used.

vii. **Principle of Enforcement** [85]**:** This principle provides that to ensure conformity with the Safe Harbor principles, there must be:

a) readily available and reasonable independent recourse mechanisms to investigate and resolve each individual's complaints and disputes, and damages are to be awarded where applicable law or private sector initiatives so provide;

---

agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

[81] *Supra* note 60.

[82] US-EU Safe Harbor Framework Principle, Access states: - *Individuals must have access to personal information about themselves that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.*

[83] US-EU Safe Harbor Framework Principle, Security states: - *Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.*

[84] US-EU Safe Harbor Framework Principle, Data Integrity states: - *Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.*

[85] US-EU Safe Harbor Framework Principle, Enforcement states :- *To ensure compliance with the Safe Harbor principles, there must be:*
(a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide;
(b) procedures for verifying that the commitments companies make to adhere to the Safe Harbor principles have been implemented; and
(c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters will no longer appear in the list of participants.

b) procedures for verifying that the commitments companies make adhere to the Safe Harbor principles have been implemented; and

c) obligations to remedy problems and sanctions must be severe enough to ensure that the organisation complies.

It was however the decision in the ***Schrems***[86] case by the *Court of Justice of the European Union* **("CJEU")** that led to the invalidation of the Safe Harbor framework.

The *Schrems* case concerned the protection of individuals when their personal data is transferred to third countries, in this case, the United States. Schrems, an Austrian citizen and long-time Facebook user, filed a complaint with the Irish data protection supervisory authority to protest the transfer of his personal data from Facebook's Irish subsidiary to Facebook Inc. and the servers in the United States, where it was processed. He contended that, in light of Edward Snowden's 2013 revelations about the surveillance activities of US surveillance services, US law and practice did not provide adequate protection for personal data transferred to US territory. Snowden revealed that the NSA tapped directly into the servers of companies such as Facebook and could read the content of chats and private messages. Transfers of data to the US were based on an adequacy decision issued by the Commission in 2000, which allowed transfers to US companies that self-certified that they would protect personal data transferred from the EU and would comply with the so-called "Safe Harbour principles." When the case was heard by the CJEU, it looked into the legality of the Commission's decision in light of the Charter. It recalled that the EU's fundamental rights protection requires derogations and limitations to those rights to apply only when absolutely necessary.

And on October 6, 2015, the CJEU ruled that the Safe Harbor framework was invalid for several reasons, including that it allowed for government interference with the directive's protections, that it did not provide legal remedies for individuals seeking access to data about them or to have their data erased or

---

[86] Maximillian Schrems v. Data Protection Commissioner [GC], CJEU, C-362/14, available at: https://curia.europa.eu/juris/liste.jsf?num=C-362/14 (Last accessed on August 28, 2020).

amended, and that it prevented national supervisory authorities from exercising their powers appropriately. Furthermore, the CJEU stated that "legislation that does not allow an individual to pursue legal remedies in order to obtain access to personal data relating to him, or to obtain the rectification or erasure of such data" is incompatible with the fundamental right to effective judicial protection[87].

2.8.2. EU-US Privacy Shield Framework:

Subsequent to the invalidation of the Safe Harbor framework by the CJEU, on July 12, 2016, the *EU-US Privacy Shield Framework*[88] was approved as a valid legal mechanism for complying with the EU requirements when transferring personal data from the EU to the US. On August 1, 2016, the Department of Commerce began accepting Privacy Shield compliance certifications, replacing the U.S.-EU Safe Harbor Framework.

Under the EU-US Privacy Shield Framework, U.S. companies must certify compliance with seven primary data security principles which were included in the Safe Harbor framework, and additionally included the responsibilities[89] to:

i. Respond to complaints within 45 days;
ii. Provide a response with consideration of the merits and potential solutions;
iii. Assign an independent dispute resolution body in the EU or the U.S.;
iv. Reply promptly to Department of Commerce requests for information;
v. Provide information to the FTC when resolving complaints.

---

[87] Charter Of Fundamental Rights Of The European Union , Article 47 states:- *Right to an effective remedy and to a fair trial :*
Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.
Available at : https://www.europarl.europa.eu/charter/pdf/text_en.pdf (Last accessed on September 05, 2020).

[88] The EU-US Privacy Shield Framework, available at: https://www.privacyshield.gov/Program-Overview, (Last accessed September 07,2020)

[89] EU-U.S. Privacy Shield Framework, Key New Requirements for Participating Companies, available at: https://www.privacyshield.gov/Key-New-Requirements (Last accessed September 07,2020)

vi. Work together with *Data Protection Authorities* **("DPA's");** and,

vii. Be subject to regular compliance audits.

Participating organisations must also agree to increased monitoring and enforcement requirements via national or local DPA's, as well as a broader role for the U.S. regulatory authorities.

Significantly, in response to the development of new technologies and revelations about mass surveillance undertaken by some states, the United Nations has adopted two resolutions on privacy issues titled "*the right to privacy in the digital age*"[90] in 2013 which strongly condemn mass surveillance and emphasise the impact it can have on fundamental rights to privacy and freedom of expression of individuals, as well as the functioning of a vibrant and democratic society.

Despite the fact that they are not legally binding, they have sparked an important international, high-level political debate about privacy, new technologies, and surveillance.

While the 2013 resolution focused on the negative effects of mass surveillance and the responsibility of states to constrain the powers of intelligence authorities, the recent resolution of 2016 of the United Nations reflect a key development in the debate on privacy in the United Nations,[91] as in addition to the responsibility of state authorities, the resolution emphasises the private sector's responsibility to respect human rights and call on businesses to inform users about the collection, use, sharing, and retention of personal data, as well as to implement transparent processing policies.

---

[90] UN General Assembly, Resolution On The Right To Privacy In The Digital Age, A/RES/68/167, New York, 18 December 2013; and UN, General Assembly, Revised Draft Resolution On The Right To Privacy In The Digital Age, A/C.3/69/L.26/Rev.1, New York, 19 November 2014, available at http://undocs.org/A/RES/68/167, (Last accessed on October 08, 2020).

[91] UN General Assembly, Revised Draft Resolution On The Right To Privacy In The Digital Age, A/C.3/71/L.39/ Rev.1, New York, 16 November 2016; and UN, Human Rights Council, The Right To Privacy In The Digital Age, A/HRC/34/L.7/Rev. 1, 22 March 2017, available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1, (Last accessed on October 10, 2020).

Thus, the Data Protection Principles establish the conditions under which personal data may be processed. If an organisation is unable to meet the Data Protection Principles (and no exemption or derogation applies), such processing is illegal. As a result, understanding these Principles becomes critical.

While many countries now have laws in place based on the principles of data protection, there is still a significant need for stronger legal safeguards to provide users with confidence in what Government and Businesses do with their personal information. Despite the fact that most countries including India recognise the importance of data protection in certain sectors, they are yet to develop comprehensive data protection legislation that applies to all business sectors and the Government.

In the ensuing chapter, the Researcher has highlighted the existing Data Protection Laws in the European Union, United States of America and the United Kingdom as it will be enlightening to examine practices followed in these jurisdictions having a robust and matured legal framework on the subject law, in determining India's approach to data protection.

CHAPTER 3 - DATA PROTECTION LAWS IN THE EUROPEAN UNION, UNITED STATES OF AMERICA AND THE UNITED KINGDOM.

3.1. INTRODUCTION:

In shaping India's approach to data protection, a review of foreign jurisdictions reveals two distinct models in the field of data protection. The *European Union* **("EU")** model and others like it including the *United Kingdom* **("UK")** provide for a comprehensive data protection law based on a rights-based approach, whereas the *United States of America* **("US")** model has sector-specific data protection laws due to each jurisdiction's unique and distinct conceptual basis for privacy.

The right to privacy is a fundamental right in the EU that aims to protect an individual's dignity. The European Charter of Fundamental Rights recognises the right to privacy as well as the right to personal data protection.[92] *The Data Protection Directive, 1995 (Directive 95/46/EC)* [93], was the first major EU legal instrument on data protection. It was heavily influenced by the OECD Guidelines[94], and it sought to achieve a uniformly high level of data protection in the EU by harmonising data protection legislation to ensure that the free flow of data was not hampered.

The EU Member States eventually adopted the Data Protection Directive, 1995 as the national legislation. Because it was a non-binding instrument, there was some leeway for interpretation. The rapidly changing data landscape prompted the EU to

---

[92] *Supra* note 70, See also *Supra* note 71.

[93] The European Union Agency for Fundamental Rights (FRA), the Council of Europe and the Registry of the European Court of Human Rights, Handbook on European Data Protection Law (2014), available at: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf, (Last accessed on November 14, 2020), See also *Supra* note 68.

[94] *Supra* note 30.

update its data protection regulatory environment and the *EU General Data Protection Regulation of 2016* (EU) 2016/679[95] is the result of this process.

3.2. EUROPEAN UNION DATA PROTECTION LAW:

The EU's data protection laws have long been regarded as a global gold standard. The EU law is divided into two parts: i.e. *primary* and *secondary* EU law. The treaties, the *Treaty on European Union* **("TEU")** and the *Treaty on the Functioning of the European Union* **("TFEU")** which has been ratified by all EU member States constitute *"primary EU law".* Whereas the EU's regulations, directives, and decisions adopted by the EU institutions given such authority under the treaties are considered as *"secondary EU law".*

Given that the European Economic Community was initially envisioned as a regional organisation focused on the economic integration and the establishment of a common market, the original treaties of the European Community made no reference to human rights or their protection.[96]

The *Lisbon Treaty* is considered as the watershed moment in the evolution of data protection law in EU, not only because it elevates the *Charter* to the status of a binding legal document at the level of primary law, but also because it provides for the right to personal data protection.

---

[95] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation**),**available at: https://gdpr-info.eu/ (Last accessed on November 20, 2020).

[96] Handbook on European Data Protection Law, 2018, available at https://fra.europa.eu/en/publication/ 2018/handbook-european-data-protection-law-2018-edition (Last accessed on November 20, 2020).

This right is expressly stated in Article 16 of the TFEU[97], which also establishes a new legal framework, granting the EU the authority to legislate on data protection issues.

This is considered to be a significant development because EU data protection rules, particularly the Data Protection Directive, were initially based on the legal basis of the internal market and the need to approximate national laws so that free movement of data within the EU was not hampered. Article 16 thus provided an independent legal basis for a modern, comprehensive approach to data protection that encompasses all areas of EU competence, including police and judicial cooperation in criminal matters and further provides that compliance with data protection rules adopted in accordance with it must be monitored by independent supervisory authorities. It served as the legal foundation for the adoption of the EU General Data Protection Regulation, 2016 which is a comprehensive reform of data protection laws in the EU.

The European Commission announced on January 25, 2012, that it would attempt to unify data protection law across a unified EU through proposed legislation known as the *General Data Protection Regulation*. The European Commission's goals for this new legislation included harmonising the 27 national (EU member states) data protection regulations into a single unified regulation, improving corporate data transfer rules outside the EU, and increasing user control over personal identifying data, and after four years of negotiations, the General Data Protection Regulation received final legislative approval on April 27, 2016, and

[97] Treaty on the Functioning of the European Union, Article 16 states:-
1. Everyone has the right to the protection of personal data concerning them.
2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.
The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

after a two-year transition period, the regulation became fully enforceable on May 25, 2018.

The *EU General Data Protection Regulation, 2018* **("EU GDPR")** is considered as one of the most significant achievements in recent years and is now acknowledged as the general data protection law throughout the EU and it replaces the 1995 Data Protection Directive, which was enacted in the EU during the early days of the internet.

3.2.1. EU General Data Protection Regulation, 2016 ("EU GDPR"):

The EU GDPR is a comprehensive data protection framework that applies to the processing of personal data by any means and to processing activities carried out by both the government and private entities, with some exceptions for national security, defence, public security, and so on[98]. Similarly, it continues to recognise

---

[98] EU GDPR, Article 23, Restrictions states:-,

1. *Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:*
    1. *national security;*
    2. *defence;*
    3. *public security;*
    4. *the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;*
    5. *other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;*
    6. *the protection of judicial independence and judicial proceedings;*
    7. *the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;*
    8. *a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);*
    9. *the protection of the data subject or the rights and freedoms of others;*
    10. *the enforcement of civil law claims.*
2. *In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:*
    1. *the purposes of the processing or categories of processing;*
    2. *the categories of personal data;*
    3. *the scope of the restrictions introduced;*
    4. *the safeguards to prevent abuse or unlawful access or transfer;*
    5. *the specification of the controller or categories of controllers;*

and enforce the OECD Guidelines core data protection principles.[99] The EU GDPR takes a rights based approach to data protection and centres the law on the individual. As a result, it imposes extensive control over the processing of personal data both during and after data collection.

Furthermore, subject to certain exceptions, the collection of certain types of personal data known as sensitive personal data (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health and sex life) is prohibited.[100] Thus, in order for processing

---

6. *the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;*
7. *the risks to the rights and freedoms of data subjects; and*
8. *the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.*

[99] *Supra* note 30.

[100] EU GDPR, Article 9, Processing of Special Categories Of Personal Data states:-

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e) processing relates to personal data which are manifestly made public by the data subject;

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health

to be lawful and fair[101], the entity collecting personal data must follow a number of principles such as purpose specification[102], data minimisation[103], data accuracy[104], security safeguards[105], and so on.

Additionally, an individual retains extensive control over their data after it has been collected. This is made possible by the legal guarantee of a wide range of individual participation rights. These include the right to confirm whether or not data about oneself is being processed[106], the right to access data[107], the right to

---

care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j)processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

[101] EU GDPR. Article 5(1)(a) states:- Principles Relating To Processing Of Personal Data:

1.Personal data shall be:

a). processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

[102] EU GDPR. Article 5(1)(b) states:- Principles Relating To Processing Of Personal Data

1. Personal data shall be:

b). collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

[103] EU GDPR. Article 5(1)(c) states:- Principles Relating To Processing Of Personal Data :

1.Personal data shall be:

c). adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

[104] EU GDPR. Article 5(1)(d) states:- Principles Relating To Processing Of Personal Data :

1.Personal data shall be:

d). accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

[105] EU GDPR. Article 5(1)(f) states:- Principles Relating To Processing Of Personal Data :

1.Personal data shall be:

f). processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

[106] EU GDPR , Article 15 states:- Right of access by the data subject :

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a)the purposes of the processing;

b)the categories of personal data concerned;

rectification of data[108], the right to data portability[109], the right to restrict processing[110], the right to erasure[111], the right to object to processing[112], including

---

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. [2]For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. [3]Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. *The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.*

[107] *Ibid* at 106.

[108] EU GDPR , Article 16 states:- Right to rectification :

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. [2]Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

[109] EU GDPR , Article 20 states:- Right to data portability :

1. *The data subject shall have the right to receive the 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 have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:*
   a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
   b) the processing is carried out by automated means.
2. *In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.*
3. *The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17.That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*
4. *The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.*

[110] EU GDPR , Article 19 states:- Notification obligation regarding rectification or erasure of personal data or restriction of processing :

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. [2]The controller shall inform the data subject about those recipients if the data subject requests it.

[111] EU GDPR, Article 18 states:- Right to Restriction of Processing :

1. *The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:*
   a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
   b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

the right to object to processing for direct marketing purposes, and the right to object to automated decisions.[113]

---

c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. *A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.*

[112] EU GDPR, Article 21 states:- Right To Object :

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. [2]The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. *Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.*

[113] EU GDPR, Article 22 states:- Automated Individual Decision-Making, Including Profiling :

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

3.2.1.1 Applicability of the EU General Data Protection Regulation:

The EU GDPR is unusual in the sense that it even applies to organisations that may have little to do with the EU.[114] For example, a US web development company based in Denver, Colorado that primarily sells websites to Colorado businesses, if the said organisation tracks and analyses EU visitors to its company's website, it will be subject to the EU GDPR's regulations. Thus, if an organisation processes the personal data of EU citizens or residents, or provides goods or services to such people, the EU GDPR will apply to the organisation even if it is not located within the EU.

Thus, the entire purpose of the EU GDPR is to protect data belonging to EU citizens and residents irrespective of the physical location of the organisation. As a result, the law applies to organisations that handle such data whether they are based in the EU or not, and this phenomenon is known as the *"extraterritorial effect"*.[115] Thus, a non-EU organisation may be required to comply with the EU GDPR in the following two scenarios, which are:

i. Providing goods or services:

An example of this scenario is, as the internet makes goods and services in remote locations available to people all over the world, if a teenager in India orders a gift from a local gift store in India online and has it delivered to a friend's house in Germany, and pays in Euro currency on the website, then even

---

[114] Available at: https://gdpr.eu/companies-outside-of-europe/ (Last accessed on September 16, 2022).

[115] EU GDPR, Article 22 states:- Territorial scope :

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. *This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.*

if though the company is not based in the EU but serves EU clients, it should strive to be EU GDPR compliant.

ii. Monitoring behaviour or actions of EU residents or citizens:

An example of this scenario is: If an organisation based outside of the EU employs web tools that allow it to track cookies or IP addresses of people visiting its website from EU countries, then the organisation is subject to the EU GDPR.

The rule of applicability of the EU GDPR regulations however has two significant exceptions. The first being, the EU GDPR does not cover "*purely personal or household activity*", so, if an organisation has gathered email addresses to organise a picnic with co-workers, it won't have to encrypt its contact information to comply with the EU GDPR. Only organisations engaged in "*professional or commercial activity*" are subject to the EU GDPR. So, if an individual is gathering email addresses from friends in order to fundraise for a side business project, then EU GDPR will apply.

The second exception applies to businesses with fewer than 250 employees. Though the EU GDPR does not completely exempt *small and medium-sized enterprises* **("SMEs"),** it does exempt them from most record-keeping obligations unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects or where the processing is not occasional or where the processing includes special categories of data or where the processing involves personal data relating to criminal convictions and offences.[116]

[116] EU GDPR, Article 30(5) states:- Records of processing activities :-
The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

3.2.1.2 Principles of the EU General Data Protection Regulation:

It is important to note that at the heart of the EU GDPR are seven key principles, which are outlined in Article 5 of the legislation and are intended to guide how individual's data can be handled. They are not hard rules, but rather an overarching framework designed to lay out the broad purposes of EU GDPR. The principles are largely based on the same as those found in earlier data protection legislation.[117]

The Seven Principles considered in the EU GDPR are:

i. **Principle of Lawfulness, Fairness and Transparency**[118] **:**

The first principle is self-evident, in the sense that organisations must ensure that their data collection practises do not violate the law and that they are not concealing anything from the data subjects i.e. the individuals.

ii. **Principle of Purpose Limitation**[119] **:**

This states that organisations should only collect personal data for a specific purpose, state that purpose clearly, and only collect data for as long as necessary to complete that purpose. Interestingly however, processing done for public interest archiving, scientific, historical, or statistical purposes is given more leeway.

iii. **Principle of Data Minimization**[120] **:**

---

[117] Available at: https://gdpr.eu/what-is-gdpr/ (Last accessed on November 29, 2020).

[118] EU GDPR, Article 5(1)(a), Principles relating to processing of personal data states:- *Personal data shall be:*
(a). processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

[119] EU GDPR, Article 5(1)(b), Principles relating to processing of personal data states:- *Personal data shall be:*
(b).collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

[120] EU GDPR, Article 5(1)(c), Principles relating to processing of personal data states:- *Personal data shall be:*

Data minimization entails organisations processing only the personal data required to achieve their processing goals. This has two major advantages. First, in the event of a data breach, the unauthorised individual will only have limited access to the data. Second, data minimisation makes it easier to maintain data accuracy and timeliness.

iv. Principle of Data Accuracy[121] **:**

The accuracy of personal data is integral to data protection. The EU GDPR mandates that every reasonable step must be taken by organisations to erase or rectify data that is inaccurate or incomplete.

v. Principle of Storage Limitation[122] **:**

The accuracy of personal data is integral to data protection. The EU GDPR provides that data must kept in a form which permits identification of data subjects only for such time period which is necessary for the purposes for which the personal data is processed. The exception provided to this is that personal data may be stored for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and is strictly subject to implementation of the appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject i.e. the individuals.

vi. Principle of Integrity and Confidentiality[123] **:**

(c). adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

[121] EU GDPR, Article 5(1)(d), Principles relating to processing of personal data states:- *Personal data shall be:*
(d). accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

[122] EU GDPR, Article 5(1)(e), Principles relating to processing of personal data states:- *Personal data shall be:*
(e). kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

The EU GDPR casts the responsibility on the organisation to protect the collected data from being mishandled, accidentally lost, or compromised. Further in the event of a cyber-attack, the organisation should use anonymisation or pseudonymisation to protect the identity of the data subject i.e. the individuals.

vii. Principle of Accountability[124]**:**

Accountability entails taking responsibility for every step of data processing, and the EU GDPR mandates that the organisation must document and justify each step for the highest level of accountability practice. It further mandates that in case of large organisation that handles complex data, it is required to automate its documentation and EU GDPR compliance system.

Thus, it can be inferred that the EU GDPR's Principles lay down certain important requirements which can be summarised are as follows:

i. That the uniform rule to apply throughout Europe, as the EU GDPR applies in all EU member States, making it easier for businesses and citizens alike.

ii. That the personal data must be used in accordance with principles of integrity. And processing must have a clear goal. Individuals, in other words, have a right to know how their data is being used and a say in the matter. Organisations must only keep personal data for as long as necessary. Furthermore, the processing must be safe and secure and the organisations must have and keep proper documentation demonstrating compliance with regulations.

iii. That the use of the personal data use must be legal. It is not legal if the processing is not done for the legal purposes. It provides that personal data processing is considered legal if it is required for contract performance or to prevent fraud and conduct marketing.

---

[123] EU GDPR, Article 5(1)(f), Principles relating to processing of personal data states:- *Personal data shall be:*

(f). processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

[124] EU GDPR, Article 5(2) states:- *Principles relating to processing of personal data*: *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*

iv. It provides that any Breach of personal data must be reported. If personal data is disclosed, accessed, changed, or stolen, it is the responsibility of the organisation to take action and repot such breach. This is applicable even if the breach has occurred at one of suppliers of the organisation and not at the organisation itself.

v. It considers that businesses are accountable to their vendors and as such the EU GDPR imposes contractual obligations on the data controller of the organisation to ensure that its suppliers comply with data protection obligations as if the supplier compromises data, the controller will be held accountable.

3.2.1.3 Role and Requirement of Data Protection Officer under the EU GDPR:

Organisations are mandatorily required by the EU GDPR to appoint a Data Protection Officer[125].The EU GDPR aims to protect personal data on the Internet and to that end, the EU GDPR requires that most organisations that handle people's personal information appoint someone to oversee the organisation's EU GDPR compliance. Thus the *Data Protection Officer* **("DPO")** is an organisation's EU GDPR focal point and must be well-versed in data protection law and practices.

An organisation may be conducting large-scale data processing even if the organisation itself is small and hiring a full-time DPO may not be feasible for smaller organisations. In such cases a DPO can be hired or shared among several smaller organisations, as long as the DPO is easily accessible to each organisation

---

[125] EU GDPR**,** Article 38 states:- *Position of the data protection officer :*

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

and can carry out its duties effectively for each of such organisation. Also, if an organisation is too large for a single DPO to handle all of the duties alone, it may be necessary to provide the DPO with support staff. The EU GDPR provides for both scenarios.

3.2.1.4 Legal Processing of Personal Data under the EU GDPR:

The EU GDPR specifies the circumstances under which it is legal to process personal data[126]. It provides that collecting, storing, or selling someone's personal data is prohibited unless it can be justified with one of the following:

i. The data subject itself has provided the organisation with specific, unambiguous permission to process the data. For example, the individual has subscribed to the organisation's marketing email list.

ii. Processing is required by the organisation to carry out or prepare to carry out a contract to which the data subject is a party. For example, in case of a property lease, before leasing property to a prospective tenant, the organisation can conduct a background check, by processing the personal data of the prospective tenant.

iii. Where the personal data was required to be processed in order to fulfill a legal obligation on the part of the organisation. For example, in the case where the

---

[126] EU GDPR, Article 6(1) states:- *Lawfulness of processing :*
1.Processing shall be lawful only if and to the extent that at least one of the following applies:
a.the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b.processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c.processing is necessary for compliance with a legal obligation to which the controller is subject;
d.*processing is necessary in order to protect the vital interests of the data subject or of another natural person*;
e.processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

organisation may receive an order from a court directing such processing or disclosure.

iv. In cases where the data was required to be processed in order to save someone's life.

v. Where processing is required in order to complete a task in the public interest or to carry out an official function. For example, processing of personal data for a public benefit scheme.

vi. Where the organisation has a legal reason to process someone's personal information. Though the EU GDPR provides that the fundamental rights and freedoms of the data subject always take precedence over the organisation's legal interests, especially if the data is that of a child.

3.2.1.5. Significance of Consent under the EU GDPR:

It is specifically provided under the EU GDPR that personal data should be processed only on the basis of the data subject's consent for the processing to be lawful .[127] The consent it is stated should be freely given, specific, informed, and unambiguous. It also provides that the consent requests must be, clearly distinguishable from other matters and must be written in clear and plain language.

---

[127] EU GDPR, Article 7 states:- Conditions for consent :

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, *the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract*

See Also : EU GDPR **,** Recital 40 states:- Lawfulness of data processing :

In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

The EU GDPR accords the data subjects the right to withdraw previously given consent at any time, and the organisation is bound respect this decision of the data subject. Further, it provides that organisations cannot simply change the processing's legal basis to one of the other justifications so as to circumvent the law. With regards to the processing of personal data of children, the EU GDPR considers that children deserve special protection when it comes to personal data because they may be less aware of the risks, consequences, and safeguards involved, as well as their rights in relation to personal data processing[128]. It specifically provides that children under the age of 16 years can only give consent with their parent's permission and the organisations are advised to keep documentary proof of such consent obtained. The EU GDPR however allows Member States to make provision by law in its legislations for a lower age, as long as it is not less than 13 years.[129] Interestingly, the EU GDPR specifies that in the context of preventive or counselling services provided directly to a child, the consent of the parent of the child should not be required.

3.2.1.6 Penalties for breach under the EU GDPR:

As the EU GDPR is designed to apply to all types of businesses, from multinational corporations to micro-enterprises, the fines for breach of the provisions of the EU GDPR are flexible and scale with the scale of the organisation. The EU GDPR also provides for imposing fine on the organisation regardless of size and organisation that is not EU GDPR compliant also faces significant liability.

---

[128] EU GDPR, Recital 38 states:- *Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. [2]Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. [3]The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.*

[129] EU GDPR, Article 8(1) states:- Conditions applicable to child's consent in relation to information society services:
Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. [2]Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. [3]Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

In terms of the EU GDPR some violations are more serious than others and as such the fines too are divided into two categories, viz :

i. It provides that less serious violations could result in a fine of up to €10 million (Euro 10 million), or 2% of the organisation's worldwide annual revenue from the previous fiscal year, whichever is greater.[130]

ii. For the more serious violations, i.e. actions of the organisation which directly contradict the EU GDPR's core principles of the right to privacy and the right to be forgotten, could result in a fine of up to €20 million (Euro 20 million), or 4% of the organisation's worldwide annual revenue from the previous fiscal year, whichever is greater.[131]

3.2.1.7 Transfers of Personal Data to Third Countries or International Organisations under the EU GDPR:

There are large amounts of cross-border transfers of personal data in today's globalised world, which are sometimes stored on servers in different countries and the EU GDPR protection travels with the data, which means that the rules protecting personal data continue to apply regardless of where the data lands.[132]

---

[130] EU GDPR, Article 83(4) states:- *General conditions for imposing administrative fines: Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:*
a. the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
b. the obligations of the certification body pursuant to Articles 42 and 43;
c. *the obligations of the monitoring body pursuant to Article 41(4).*

[131] EU GDPR, Article 83(5) states:- *General conditions for imposing administrative fines: Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:*
a. the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
b. the data subjects' rights pursuant to Articles 12 to 22;
c. the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
d. any obligations pursuant to Member State law adopted under Chapter IX;
e. *non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).*

[132] EU GDPR, Article 44 states:- *General principle for transfers: Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller*

This is also true when data is transferred to a country that is not a member of the EU (referred to as a **"third country"**).

The EU GDPR provides that data transfers from the EU to a third country is permitted when the said third country is declared as providing an adequate level of protection through a *European Commission* decision **("Adequacy Decision")**[133], **,**

---

and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

[133] EU GDPR, Article 45 states:- *Transfers on the basis of an adequacy decision :*

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the

which means that data can be transferred to another organisation in that third country without the data being compromised or be subjected to additional conditions. In other words, transfers to an "*adequate*" third country will be comparable to data transmissions within the EU.

The EU GDPR also provides that, in the absence of an adequacy decision, a transfer of personal data can take place only if the controller or processor of such data has provided appropriate safeguards, and on condition that data subject rights enforceable and effective legal remedies for data subjects are available. [134]

---

decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

[134] EU GDPR, Article 46 states:- Transfers subject to appropriate safeguards :

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

The appropriate safeguards in terms of the EU GDPR for transfer of personal data are:

i. organisations can transfer personal data based on binding corporate rules in the case of a group of undertakings or groups of companies engaged in a joint economic activity with the recipient of personal data, for example, using European Commission approved standard contractual clauses, and;

ii. Adhering to a code of conduct or a certification mechanism, as well as obtaining binding and enforceable commitments from the recipient to apply appropriate safeguards to protect the transferred data.

Nevertheless, for transfer of personal data to a third country that is not the subject of an adequacy decision, and where appropriate safeguards are lacking, can be made based on a number of derogations for specific situations, such as where an individual has explicitly consented to the proposed transfer after being provided with all necessary information about the risks relating to the transfer.[135]

---

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

[135] EU GDPR, Article 49(1) states:- *Derogations for specific situations,*

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data

3.2.1.8 Grievance redressal mechanism under the EU GDPR:

The EU GDPR provides for an effective grievance redressal mechanism in case of breach or infringement the data protection provisions, thus under the EU GDPR an aggrieved person has three options if the individual believes that his/her data protection rights have been violated:

i. the individual has the option to file a complaint with the his/her country's *Supervisory Authority* i.e. *the Data Protection Authority* ***("*DPA")***[136] within three months, and the authority is required to investigate and inform the aggrieved person of the progress or outcome and legal action taken against the company or organisation.

ii. alternately, the aggrieved person can file a direct court action against the organisation which is believed to have violated his/her data protection rights and importantly this does not preclude the aggrieved person from filing a complaint with the national DPA, if so desired.[137]

---

subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

[136] EU GDPR, Article 51states,**:-**Supervisory authority :

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

[137] EU GDPR, Article 77 states**:-** Right to lodge a complaint with a supervisory authority :

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

iii. if the aggrieved person believes that the DPA has not handled the complaint correctly, or if aggrieved person is dissatisfied with its response, or if the DPA has not informed aggrieved person of the progress or outcome of the complaint within three months of the date of lodging the complaint, the aggrieved person can file a direct action against the DPA in the court of law.[138]

iv. without prejudice to the other available administrative or non-judicial remedy, each aggrieved person has the right to an effective judicial remedy by initiating legal proceedings against a controller or processor in the courts of the member State in which the controller or processor has an establishment, or alternatively, such proceedings may be initiated in the courts of the member State in which the aggrieved person resides, unless the controller or processor is a public authority of a member State acting in the exercise of its public powers.[139]

3.2.1.9 Independence of the Supervisory Authority:

A *Supervisory Authority* also known as a *Data Protection Authority* **("DPA")** under the EU GDPR is an independent public authority, which oversees the application of European data protection law through investigative and corrective powers.

---

[138] EU GDPR**,** Article 78 states:- Right to an effective judicial remedy against a supervisory authority :
1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.
2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.
3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.
4. *Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.*

[139] EU GDPR **,** Article 78 states:- Right to an effective judicial remedy against a controller or processor:
1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.
2. *Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.*

The DPA's offer expert advice on data protection matters and address complaints about violations of EU GDPR and applicable national laws. Each EU member country has one DPA and the EU Charter grants all EU citizens the constitutional right to file a complaint regarding their right to data protection.[140]

In the light of the above, when compared to the evolving series of European frameworks, directives, and regulations, the newly enacted EU GDPR becomes clear. Though the EU GDPR's requirements may appear onerous or unnecessary to some, but when compared to the previous patchwork of European law and policy in this area, the EU GDPR is expected at the very least to facilitate a more uniform international effort regarding data protection and compliance. Nevertheless the EU GDPR is criticised for its lack of effectiveness and uneven implementation. Despite the large fines, privacy and civil rights the EU GDPR has failed to achieve its intended goal of protecting European citizens' data, particularly from large tech companies. It is argued that inspite of the strict regulation of the EU GDPR, Big Tech companies have failed to limit targeted advertising. For example, the Company *Meta Ireland* introduced "contractual necessity", in its updated, privacy-focused terms of service for Instagram and Facebook that sought to legitimise the processing of user data.

---

[140] EU GDPR **,** Article 52 states:- Independence:
Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.
1. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
2. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.
3. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.
4. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.
5. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

It is also noted that the EU GDPR has done little to assist public and private sector organisations in dealing with privacy issues arising from on emerging digital technologies. For example, The technological industry's growing reliance of the tech industry on emerging AI technologies, as exemplified by Open AI's popular ChatGPT chat bot, has the potential to exacerbate privacy concerns, though Member States of the EU have brought some AI-related cases against organisations for facial recognition technology, video surveillance, and political campaigns, the EU GDPR proves inadequate to address these growing threats and an EU AI law is still years away. Moreover the fragmented implementation of the EU GDPR remains a challenge, however the fact that the EU GDPR can sanction non-EU tech companies can be viewed as a sign of its success.[141]

Nevertheless though it is too early to tell whether the EU GDPR's reporting, compliance, and enforcement provisions will work as intended, it is expected that other global regulations are likely to follow suit soon.

3.3. PRIVACY LAWS IN THE UNITED STATES OF AMERICA:

In the *United States* **("US")**, privacy protection is essentially a form of liberty protection, or the protection of one's personal space from the Government. Thus, in the US, the right to be left alone has come to represent a desire for as little Government intervention as possible. While there is no explicit provision in the US Constitution granting a right to privacy, the right is reflected in a limited manner in the Fourth Amendment to the US Constitution i.e. *the right against unreasonable searches and seizures*. However, US courts have collectively acknowledged the

[141] 5 Years of GDPR: Criticism Outweighs Positive Impact, available at: https://www.bankinfosecurity.com/-a-22156#:~:text=GDPR%2C%20which%20went%20into%20effect,a%20company's%20global%20annual%20turnover (Last accessed on 26 November, 2023).

right to privacy by piecing together the limited privacy protections reflected in the US Constitution's First, Fourth, Fifth, and Fourteenth Amendments.

Apart from the dissimilarity in the conceptual basis of privacy, the US approach to privacy and data protection differs from that of the EU in a number of ways. Firstly, unlike in the EU, the US lacks a comprehensive set of privacy rights/principles that address the use, collection, and disclosure of data, instead there are industry specific regulations. Secondly, the approach to data protection differs between the public and private sectors.

Thus, there are two distinct trends in the US approach to data protection viz: stringent norms for Government processing of personal information, and notice and choice based models for private sector data processing. This dichotomy can be attributed largely to the *laissez faire* culture of US markets, as opposed to the rights centric culture of EU markets.[142]

The organisations operating in the US are required to comply with both the Federal and State laws in order to comply with US data privacy laws as it is the Federal statutes that generally govern the collection, storage, and use of sensitive non-public personal information, whereas State laws, on the other hand, generally govern disclosure requirements following a security breach involving non-public personal information.

Further, the Federal statutes can be enforced by the Federal Government Regulators or, if they include a private right of action, by individuals affected in civil suits. State laws on the other hand are enforced by State Government Regulators or, in the case of a private right of action, by private citizens bringing civil suit.[143]

---

[142] Justice B.N.Srikrishna Commission, White Paper of The Committee of Experts on A Data Protection Framework For India, available at: https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf(Last accessed on September 21, 2021).

[143] Robert Hasty, Dr. Trevor W. Nagel and Mariam Subjally, White and Case, Data Protection Law in the USA .Advocates for International Development, August 2013, available at: https://web.archive.org/web/20150925093457/http://www.a4id.org/sites/default/files/user/Data%20Protection%20Law%20in%20the%20USA_0.pdf (last accessed on September 23, 2021).

3.3.1 US Federal Laws:

In the United States, Federal data protection laws are primarily influenced by industry and data type, there are numerous laws aimed at strengthening privacy systems and reducing unfair or deceptive practises in society. Furthermore, they emphasise the importance of protecting children's online privacy as well as overall fraud and abuse prevention in society. With a greater emphasis on data privacy and consumer protection in recent years, it is likely that regulators will enforce data protection laws more strictly in the near future.[144]

The relevant Federal Laws regulating data protection in the US are as under:

3.3.1.1 Fair Credit Reporting Act, 1970 ("FCRA"):

The *Fair Credit Reporting Act, 1970* **("FCRA")** safeguards consumer reporting agencies information, such as credit bureaus, medical information companies, and tenant screening services in the US. The consumer report information prepared by these agencies may not be provided to anyone who does not have a purpose specified under this Act. Also companies that provide information to consumer reporting agencies face additional legal obligations, such as the obligation to investigate disputed information. Furthermore, anyone who uses the information for credit, insurance, or employment purposes must notify the affected consumer if any adverse action is taken based on such report.

The *Fair and Accurate Credit Transactions Act* supplemented this Act with numerous provisions, the majority of which dealt with record accuracy and identity theft.[145]

---

[144] U.S.Data Laws: A Comprehensive Guide to federal and State Privacy Laws, available at: https://helpy.io/blog/usa-data-laws/ (Last accessed on September 23,2021).

[145] The Fair and Accurate Credit Transactions Act, 15 U.S.C. §§ 1681-1681x, available at: https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act (Last accessed on September 23, 2021).

3.3.1.2 The Family and Educational Rights and Privacy Act, 1974 (“FERPA”):

The *Family and Educational Rights and Privacy Act* **(“FERPA”)** is a US federal law that applies directly to educational institutions, including public and private schools. This Act governs payments and student record retention at all federally recognised educational institutions. This privacy law prohibits educational institutions from using personal student information without the student's permission. Under this Act, if the student is under the age of 18 years, the educational institute must obtain the parent's permission before disclosing any personally identifiable information of the student contained in the educational records.

This Act safeguards the information contained in students' educational records and applies to all educational agencies and institutions that receive federal funding, including non-profit educational institutions. This Act considers records, files, documents, and other materials containing information directly related to a student and kept by an educational agency or institution or a person acting on their behalf as “*educational records*”. Any public or private agency or institution that receives funds under any applicable Government programme is considered an “*educational agency or institutio*n”.

The FERPA further provides that, any school that receives government educational funding must give parents of students, or students over the age of 18 years, the right to inspect and review the student's educational records, and each educational agency or institution is required to establish appropriate procedures for granting such requests within a reasonable time, but no later than 45 days after such request is made.

Furthermore, FERPA requires that if an educational agency or institution wishes to publish "Directory Information" relating to a student's name, address, telephone number, date and place of birth, field of study, activities, dates of attendance,

degrees, awards, and institution attended by the student, the agency or institution must first give public notice of the categories of information it intends to make public and allow a reasonable time for a parent to notify the agency or institution that it intends to inform the agency or institution that it intends to inform the agency or institution.

Finally, educational agencies or institutions are required under FERPA to keep records that identify all individuals, agencies, or organisations that have requested or obtained access to a student's records, as well as the interest that each third-party has in requesting such information. This record must be accessible only to parents, school officials, and individuals in charge of keeping such records. And importantly such personal information can only be transferred to third parties on the condition that no other party has access to it.

FERPA however does not provide for a private cause of action, however, its provisions may be enforced by the Secretary of Education. [146]

3.3.1.3 United States Privacy Act, 1974:

To improve individual privacy protection, the Federal Government enacted the United States Privacy Act in 1974. This Act established the rules and regulations for the collection, use, and disclosure of personal information by US Government agencies. The following are some of the rights guaranteed to the citizens under the United States Privacy Act:

i. **The right to request access and correct data if necessary:** Under this Act, citizens of the US have the right to access their personal data held by Government agencies and request changes if they believe the information is inaccurate.

[146]The Family Educational Rights and Privacy Act, available at: https://www.govinfo.gov/content/pkg/USCODE-2011-title20/pdf/USCODE-2011-title20-chap31-subchapIII-part4-sec1232g.pdf, (Last accessed on September 28, 2021).

ii. **The right to data access (restricted on an individual basis):** Government agencies under this Act, are authorised to grant data access to users based on their role in their company.

iii. **The right to information about uses of data:** Individuals under this Act have the right to know how the Government agencies use their personal information.[147]

3.3.1.4 Computer Fraud and Abuse Act, 1986 ("CFAA"):

To address the growing menace of computer hacking, the *Computer Fraud and Abuse Act, 1986* **("CFAA")** was enacted. It has been amended several times over the years, most recently in 2008, to cover a wide range of conduct far beyond its original intent. The CFAA forbids intentionally gaining unauthorised or excessive access to a computer in the US.

The CFAA was designed to prevent unauthorised access to computers of federal interest. The amendment to this Act increased the penalties for fraud and related activities involving access devices and computers, as well as increased protection for federal interest computers, and attempted to limit federal jurisdiction over computer crimes to cases involving a compelling federal interest i.e. where computers of the Federal Government or certain federal agencies are involved or where the crime itself is interstate in nature.

The 1994 amendment to the CFAA expanded the scope of prohibited conduct to include transmissions, specifically prohibiting, knowingly causing the transmission of a programme, information, code, or command that intentionally causes damage without authorisation. With these changes, the statute's emphasis shifted from a

[147] U.S. Privacy Laws: The Complete Guide, Available at : https://www.varonis.com/blog/us-privacy-laws, (Last accessed on September 24, 2021).

technical concept of computer access and authorisation to the perpetrator's malicious intent and resulting harm.[148]

3.3.1.5 Electronic Communications Privacy Act, 1986 ("ECPA"):

The US "Stored Wire Electronic Communications Act" and the "Electronic Communications Privacy Act" are commonly referred to as the *Electronic Communications Privacy Act, 1986* **("ECPA")**. The ECPA supplemented the "Federal Wiretap Act,1968", which addressed interception of conversations over 'hard' telephone lines but did not cover computer and other digital and electronic communications. Several subsequent pieces of legislation, including the USA Patriot Act, clarified and updated the ECPA to keep up with the evolution of new communications technologies and methods, including, in some cases, relaxing restrictions on law enforcement access to stored communications. The ECPA thus safeguards wire, oral, and electronic communications while they are being made, in transit, and stored on computers. The Act also covers email, phone conversations, and electronic data storage.[149]

3.3.1.6 The Video Privacy Protection Act, 1988 ("VPPA"):

The *Video Privacy Protection Act, 1988* **("VPPA"),** is a Federal law that was enacted to prohibit the disclosure of personally identifiable information in connection with "pre-recorded video cassette tapes or similar audio visual material". The primary purpose of this Act is to preserve privacy with respect to the rental, purchase, or delivery of video tapes or similar audio-visual materials in the US.

While video cassettes, tapes, and other such recording materials have largely been rendered obsolete today in the midst of our current digital age, the VPPA remains

---

[148] The Computer Fraud and Abuse Act, available at: https://www.nacdl.org/Landing/ComputerFraudandAbuseAct (Last accessed on September 27, 2021).

[149] The Electronic Communications Privacy Act, available at https://bja.ojp.gov/program/it/privacy-civil-lties/authorities/statutes/1285 (Last accessed on September 26, 2021).

one of the most important means by which American consumers can protect themselves against the specific forms of data collection.

The disclosure of video rental records containing personally identifiable information is prohibited under the VPPA, with some exceptions, which are as under:

i. direct disclosure to the consumer.

ii. disclosure authorised with a consumer's written consent.

iii. disclosure made in response to a Federal criminal warrant, an equivalent State warrant, a grand jury subpoena, or a court order issued in accordance with specified guidelines.

iv. disclosure to any person if such disclosure is solely the names and addresses of consumers, and the consumer has had the opportunity to prohibit such disclosure.

v. disclosure to any person if such disclosure is incidental to the video tape service provider's ordinary course of business and,

vi. disclosure made in accordance with a civil court order.

The VPPA, in addition to limiting the circumstances under which personal information relating to an individual's video records can be legally disclosed makes any video tape service provider that discloses rental information outside the ordinary course of business liable for up to $2500 (US Dollar 25,000) in actual damages and also allows any person who is harmed by a violation of this Act to file a civil action for monetary damages.

While the VPPA was originally enacted to address rental records pertaining to physical copies of media such as video or cassette tapes, the provisions of the law still continue apply to all forms of personal information that can be derived from a person's rental history, regardless of the physical form of said rentals.[150]

[150] The Video Privacy Protection Act , 1988, available at: https://www.congress.gov/bill/100th-congress/senate-bill/2361 (Last accessed on October 05, 2021).

3.3.1.7 Telephone Consumer Protection Act, 1991 ("TCPA"):

The *Telephone Consumer Protection Act* **("TCPA")** was enacted in 1991 in response to an increase in unregulated and harassing telemarketing calls and faxes. The TCPA prohibits telephone solicitation (i.e. telemarketing) and the use of automated phone equipment in the US. It restricts the use of pre-recorded voice messages, automatic dialling, SMS, and fax communications. It mandates that the companies follow strict solicitation rules without explicit customer consent, solicitors must honour the *National Do Not Call Registry*, and subscribers may sue a company that does not follow the TCPA guidelines. Under the TCPA, consumer consent is an essential component.[151]

Telemarketers/solicitors who do not have prior consent from call or message recipients are subject to the following TCPA restrictions:

i. Telemarketers and solicitors are not permitted to call residents using a recorded or artificial voice.

ii. They are not permitted to call residents between the hours of 8 a.m. and 9 p.m. local time.

iii. They must provide their name, the name of the person or entity they are calling on behalf of, and a phone number or address for that person or entity.

iv. Telemarketers are not permitted to make automated or pre-recorded calls to emergency phone lines (911 or hospitals), doctors' offices, mobile phones, or any other recipient who will be charged for the call.

v. It is also illegal to autodial two or more lines from the same company.

vi. They are not permitted to send unsolicited faxes containing advertising.

vii. Telemarketers and solicitors must keep company-specific do-not-call lists of recipients who do not want to be called and honour those lists for five years, as well as the *National Do Not Call Registry*.

---

[151] Telephone Consumer Protection Act, available at: https://www.congress.gov/bill/102nd-congress/senate-bill/1462#:~:text=Telephone%20Consumer%20Protection%20Act%20of%201991%20%2D%20Amends%20the%20Communications%20Act,a%20hospital%2C%20medical%20physician%20or (Last accessed on September 26, 2021).

The TCPA also establishes penalties for breaking such rules. A subscriber, for example, may sue for $500 (US Dollar 500) for each violation or seek further damages, an injunction, or both. Subscribers can seek three times of the specified damages for each instance of wilful TCPA violation.[152]

3.3.1.8 The Federal Trade Commission Act, 1994 ("FTC"):

The Federal Trade Commission Act **("FTC Act")** is the primary statute of the US Federal Trade Commission. Under this Act, the Commission is empowered to, (a) prevent unfair methods of competition and unfair or deceptive acts or practises in or affecting commerce, (b) seek monetary redress and other relief for conduct injurious to consumers, (c) prescribe rules defining with specificity the unfair or deceptive acts or practises, and establishing requirements designed to prevent such acts or practises, (d) gather and compile information and data and, (e) make reports and legislative recommendations to the US Congress and the public. [153]

The FTC Act broadly empowers the U.S. Federal Trade Commission **("FTC")** to take enforcement actions to protect consumers against unfair or deceptive practices and to enforce federal privacy and data protection regulations. Accordingly, as per the FTC "deceptive practices" include a company's failure to comply with its published privacy promises and its failure to provide adequate security of personal information, in addition to its use of deceptive advertising or marketing methods.

The FTC has mandates the applicability of the following principles to the organisations for processing of personal data:

i. **Transparency**: The FTC has issued guidelines espousing the principle of transparency, recommending that organisations: (i) provide clearer, shorter, and more standardised privacy notices that enable consumers to better comprehend privacy practices; (ii) provide reasonable access to the consumer

[152] *Ibid* at 148.

[153] Federal Trade Commission Act, available at: https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act,(Last accessed on September 24, 2021).

data they maintain that is proportionate to the sensitivity of the data and the nature of its use; and (iii) expand efforts to educate consumers about commercial data privacy practices.

ii. **Lawful basis for processing**: While there is no "lawful basis for processing" requirement under U.S. law, the FTC recommends that businesses provide notice to consumers of their data collection, use and sharing practices and obtain consent in limited circumstances where the use of consumer data is materially different than claimed when the data was collected, or where sensitive data is collected for certain purposes.

iii. **Purpose limitation**: The FTC recommends privacy-by-design practices that include limiting data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law.

iv. **Data minimisation**: The FTC recommends practices for minimizing the data collection limiting it to the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law.

v. **Proportionality**: The FTC recommends practices for collecting the data and limiting it to the proportionality of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law.

vi. **Retention**: The FTC recommends privacy-by-design practices that implement "reasonable restrictions on the retention of data", including disposal once the data has outlived the legitimate purpose for which it was collected.[154]

A participating company's failure to comply with these Principles may violate Section 5 of the FTC Act's prohibition on unfair and deceptive acts. The FTC is

---

[154] F.Paul Pittman, Abdul Hafiz and Andrew Hamm, Data Protection Laws and Regulations USA, 2023, July 20, 2023, available at: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (Last accessed on November 26,2023).

committed to vigorous enforcement of the DPF Principles, and works with privacy authorities in the EU to protect consumer privacy on both sides of the Atlantic.

3.3.1.9 The Health Insurance Portability and Accountability Act, 1996 ("HIPAA"):

The *Health Insurance Portability and Accountability Act, 1996* **("HIPAA"),** is a US federal privacy protection law that protects a US citizen's medical information. HIPAA covers all entities that handle "Protected Health Information" **("PHI")** of the individuals, such as healthcare providers, hospitals, and insurance companies.

Individuals under HIPAA have the following rights when a company shares PHI with a healthcare provider or covered entity:

i. **The Right of Access:** the HIPAA provides individuals with a legal, enforceable right to see and receive copies, upon request, of the information in their medical and other health records maintained by their healthcare providers and health plans. This right is known as the HIPAA Right of Access.

ii. **The Right to Amend PHI :** a patient is given the right to amend the PHI or a record about the individual in a designated record set, for as long as the PHI is in a designated record set.[155]

The Act also provides that the patient data can be used by the covered entity only for specific purposes, such as, treatment and payment. Any marketing activities, on the other hand, necessitates that healthcare providers seek permission from patients who own their personal information. The healthcare provider must provide the patient with a notice of privacy practices outlining how the provider intends to use and protect the patient's data and importantly the patient can ask

---

155 HIPAA Patient Right Explained, available at: https://compliancy-group.com/hipaa-patient-rights/ (Last accessed on September 29,2021).

healthcare providers to limit how they use and disclose their personal information.[156]

3.3.1.10 The Gramm-Leach-Bliley Act, 1999 ("GLBA"):

The *Gramm-Leach-Bliley Act* **("GLBA")** aims to protect the financial privacy of consumers in the US. Its provisions limit when a financial institution may disclose non-public personal information about a consumer to unaffiliated third parties.

The law applies to a wide range of financial institutions, including many non traditional financial institutions. The financial institutions must inform their customers about their data-sharing practices and inform them of their right to "*opt-out*" if they do not want their information shared with certain unaffiliated third parties. Furthermore, the Act provides that any entity that receives consumer financial information from a financial institution may be restricted in its reuse and re-distribution of that information.

Under the GLBA, a "financial institution" is an entity that engages in an activity that is "financial in nature" or "incidental" to such financial activities as described in the *Bank Holding Company Act of 1956.* Thus, these are companies that bring buyers and sellers together, and then the parties negotiate and close the deal themselves, mortgage lenders, payday lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, credit counsellors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors are some examples of financial institutions under the GLBA.

The GLBA Safeguards Rule amendment, 2021 added a new instance of a financial institution i.e. "finders", these are companies that bring buyers and sellers together, and then the parties negotiate close the deal themselves.[157]

---

[156]The Health Insurance Portability and Accountability Act, available at: https://www.ncbi.nlm.nih.gov/books/NBK9573/ (Last accessed on September 29, 2021).

The Act provides that to protect individuals' privacy, financial institutions must take the following steps:

i. customers should be informed about information sharing practices and given the option to opt-out of having their data shared with third parties.

ii. The financial institutions should adhere to established guidelines for its collection, use, and protection of customer data, including online information.

iii. The financial institutions should create and implement a written information security programme to guard against unauthorised access to customer data.[158]

Importantly, the GLBA applies to financial institutions that fall under the jurisdiction of the US Federal Trade Commission but are not subject to the enforcement authority of another regulator.

3.3.1.11 Children's Online Privacy Protection Act, 2000 ("COPPA"):

The *Children's Online Privacy Protection* Act, *2000* **("COPPA")** was enacted to protect the online privacy of minors under the age of 13 years. COPPA applies to any website or online service in the US that collects, uses, or discloses personal information about children. Thus, in terms of this Act, websites and online services must take the following steps to protect children's privacy:

---

[157] The Gramm-Leach-Bliley Safeguards Rule, 16 CFR 314.2(h) states*:- Financial institution, means any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956,* See also, Bank Holding Company Act of 1956, 12 U.S.C. 1843, Section 4(k) states:- *An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.*

Financial institution does not include:

(i) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 et seq.);

(ii) The Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.);

(iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as *such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party other than as permitted by §§ 313.14 and 313.15; or*

(iv) Entities that engage in financial activities but that are not significantly engaged in those financial activities, and entities that engage in activities incidental to financial activities but that are not significantly engaged in activities incidental to financial activities.

[158] The Gramm-Leach-Bliley Act, available at: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf , (Last accessed September 28, 2021).

i. post a clear and concise privacy policy outlining what information it will collect from children, how it will be used, and under what conditions it will be disclosed to third parties.
ii. before collecting, using, or disclosing personal information from children, obtain parental consent.
iii. allow parents to review and delete personal information about their children.[159]

COPPA gives States and certain Federal Agencies the authority to enforce compliance with respect to entities over which they have jurisdiction, and it is the US FTC which enforces COPPA violations under this Act. A court can hold operators who violate the Act liable for civil penalties of up to $50,120 (US Dollar 50,120) per violation.[160]

3.3.1.12 Non-Solicited Pornography and Marketing Act, 2003 ("CAN-SPAM Act"):

The *Non-Solicited Pornography and Marketing Act, 2003* **("CAN-SPAM Act")** governs commercial email messages. Under this Act, "Commercial email messages" are email messages whose primary purpose is the commercial service or product. Email's that contain "transactional or relationship message" are not considered as commercial email message and are not subject to the CAN-SPAM Act's provisions.

This Act prohibits organisations from sending emails that contain materially false, misleading, or deceptive information in the header or subject line of the email. Thus, if an email is an advertisement or solicitation, it must clearly identify itself, it should contain "clear and conspicuous" notice of opportunity i.e. option, to opting

---

[159] The Children's Online Privacy Protection Act, available at: http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim (Last accessed on September 24, 2021).

[160] History of COPPA & GDPR Violations, Available at: https://www.privo.com/history-of-coppa-violations#:~:text=The%20FTC%20enforces%20COPPA%20violations,over%20which%20they%20have%20jurisdiction (Last accessed on September 24,2021).

out of receiving future emails from the sender, and it must include some type of return email address or other mechanism through which the recipient can opt-out and the sender must respect the recipient's decisions to opt out of receiving future emails from the sender. The Act further requires that the sender's physical postal address must be included in the email.

The CAN-SPAM Act, despite its name, does not only apply to bulk email, it applies infact to all commercial messages, which are considered by this law as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service", including email promoting content on commercial websites. This means that all emails, such as even a message to former customers announcing a new product line, must adhere to the law.

Each violation of the CAN-SPAM Act is punishable with imprisonment upto 5 years or by a fine of up to $16,000 (US Dollar 16,000) per email, or both[161]and also has considerable public relations and reputational consequences for the sender, so noncompliance can prove to be costly.

3.3.2. US State Laws:

Almost every State in America has enacted some form of data privacy law that applies to its territory. While Federal data privacy laws apply, the respective State Attorney General may sue for violations of State data privacy law as well. As a result, Federal and State statutes should not be regarded as two distinct jurisdictional spheres, but rather as sets of laws that must be applied in tandem. In most US States, data privacy law focuses on breach notification, with entities required to notify consumers whose personal information has been compromised.

---

[161] Non Solicited Pornography and Marketing Act of 2003, Sec. 5(5) states:- *Penalty:*
Whoever knowingly violates paragraph (1) shall be fined under title 18, United States Code, or imprisoned not more than 5 years, or both.

The States of California and Massachusetts have more proactive and far-reaching laws and regulations in place. It is worth noting that California and Massachusetts have passed legislations that apply to any entity with access to non-public information about one of their residents, anywhere in the US and because of the forward-thinking nature of both California and Massachusetts data privacy laws, they are included as a primary focus in this research and can provide a good indication of the maximum requirements of data privacy law compliance in the United States.

3.3.2.1 California:

In terms of data privacy, the State of California is regarded as a national leader in the United States. An organisation may find itself complying with data privacy regulations emerging in other state jurisdictions by complying with California data privacy regulations. The relevant California data privacy regulations are as under:

i. California Shine the Light Law, 2003:

The Shine the Light Act is a consumer privacy law in California. It requires businesses to disclose to a resident, upon request, what personal information about that person the business has shared with third parties and which third parties have received the personal information.

It applies to all businesses that have an established personal, family, household, or business relationship with a California resident consumer and have disclosed personal information about that consumer to third-party companies for direct marketing purposes. The Act however does not apply to businesses with fewer than 20 employees or that already comply with the *California Financial Information Privacy Act*.[162]

[162] California Civil Code §§ 1798.83(c)(1) and 1798.83(h), available at; https://codes.findlaw.com/ca/civil-code/civ-sect-1798-83.html, (Last accessed on October 17, 2021).

For this Act to apply, a business relationship must have been established through two- way communication between the business and the consumer. The business relationship ends if the consumer terminates it, or after 18 months of no further activity by the consumer on the business's product or service. A business entity is required to comply with a consumer's request if the business has disclosed the consumer's personal information to a third party within the previous 12 months.[163] There are however some exceptions to when the disclosure of a consumer's personal information is covered by Shine the Light, which are as under :

(a).personal information is being processed for purposes other than direct marketing (b).if there is a pre-existing relationship, businesses can use first-party marketing to reach out to consumers (c). keeping or servicing the customer's account (d). real estate information on the public record (e). offering a product or service jointly with contractual restrictions (f). credit history (g).for payment purposes (h).if businesses have a consumer relationship, they have an agency relationship (j).if businesses have a relationship with the consumer, use of credit or loyalty card.[164]

The Shine the Light law imposes a civil penalty of up to $500 per violation and a criminal penalty of up to $3,000 for wilful, intentional, or reckless behaviour, as well as attorney fees and costs.[165]

ii. California Financial Information Privacy Act, 2004 ("CFIPA") :

The *California Financial Information Privacy Act, 2004* **("CFPIA")** forbids financial institutions from sharing or selling personally identifiable non-public information without the consent of the consumer.

---

[163] The California Privacy Laws Explained, available at : https://www.datagrail.io/blog/data-privacy/california-privacy-laws-explained/, (Last accessed on October 17, 2020).
[164] Ibid at 186.
[165] *Supra* note 185.

The CFPIA is applicable to a financial institution doing business in the State of California and encompasses the financial activities permitted by the GLBA. To share any “non-public” personal information with an unaffiliated third party, the financial institution must first obtain written consent from the consumer that is dated and signed, and clearly and conspicuously states that by signing, the consumer consents to the disclosure of his or her non-public personal information to third parties. The form must also state that if consent is given, it can be revoked or modified at any time, and it must include information on how to do so.

The CFPIA considers "non-public personal information" as personally identifiable information that is either: (a) provided by a consumer to a financial institution, (b) obtained as a result of any transaction with the consumer or any service performed for the consumer, or (c) obtained by the financial institution in any other way.

To share any non-public personal information with an affiliated party, the financial institution must notify the consumer in writing annually that the non-public personal information may be disclosed to an affiliate and that the consumer has not directed that disclosure.

The CFPIA applies to those involved in the activities of micro-lending, community lending services, local or international banking, budgeting, or investment training initiatives, social impact investing or social impact bonds, and other actions that require the organisation to directly hold securities.

Regardless of the amount of damages suffered by the consumer, the penalties for negligent disclosures or sharing in violation of CFIPA are a civil penalty of not more than $2,500 (US Dollar 2,500) per violation, with a maximum penalty of $500,000 (US Dollar 500,000) if the disclosure or sharing results in the release of non-public personal information of more than one individual and if

the sharing causes identity theft, it provides for the civil penalties to be doubled.[166]

iii. California Online Privacy Protection Act, 2004 ("CalOPPA") :

The *California Online Privacy Protection Act* **("CalOPPA")** was the first State law in the US to require commercial websites and online services to post a privacy policy. This Act came into effect in 2004 and was amended in 2013 to require new privacy disclosures regarding online tracking.

CalOPPA applies to any person or company in the United States and potentially the rest of the world, whose website collects personally identifiable information from California residents. CalOPPA requires the website to include a prominent privacy policy that specifies what information is collected and with whom it is shared.[167]

To be in compliance with CalOPPA, the website privacy policy must (a) identify the categories of personal information collected, (b) identify all third parties with whom the operator may share personal information, (c) describe the process, if any, for customers to review and request changes to the personal information collected, and (d) identify the privacy policy's effective date.

Interestingly, CalOPPA contains no enforcement provisions and is enforced through *California's Unfair Competition Law* **("UCL")**. The California Attorney General's Office, District Attorneys, and some city and county Attorneys can sue businesses under the UCL for "unfair competition", as a result, CalOPPA violations may be considered UCL violations.[168]

---

[166] What is 'CalFIPA'?, Golden Data Law, Available at : https://medium.com/golden-data/what-is-calfipa-ee7e48c88dd0, (Last accessed on October 17, 2021).

[167] The California Online Privacy Protection Act (CalOPPA), Available at: https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/ (Last accessed on October 07, 2021).

[168] California Legislative Information, available at: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=17200.&lawCode=BPC (Last accessed on October 07, 2021).

The UCL provides that private plaintiffs may file private claims under the UCL for violations of CalOPPA, and Government officials suing for CalOPPA violations may seek civil penalties and equitable relief under the UCL. Operators who violate CalOPPA may also face action from the US Federal Trade Commission, which may take enforcement action against businesses whose posted privacy policies are deceptive i.e. when a business fails to comply with its posted privacy policy.[169]

iv. The California Consumer Privacy Act, 2018 ("CCPA"):

Following in the footsteps of the European Union's GDPR, the State of California has introduced the *California Consumer Privacy Act, 2018* **("CCPA")** which incorporates the EU's data privacy efforts into the US legislation, ushering in a new era in American digital regulation.

The CCPA gives consumers more control over the personal information that businesses collect about them, and the regulations outline how to put the law into effect. This landmark law grants California consumers new privacy rights, including, (a) the right to know what personal information a company collects about them and how that information is used and shared (b)the right to have their personal information deleted (with some exceptions) (c) the ability to refuse the sale of their personal information; and (d) The right to be treated fairly when exercising their CCPA rights.

It is important to note that the CCPA applies to all businesses and parties that collect data from California residents, regardless of the business's headquarters. Furthermore, businesses that handle the personal information of 4 million or more customers face additional legal obligations.

---

[169] *Ibid* at 164.

This Act also includes a new category of protection for sensitive data and the California Attorney General is given the regulatory and enforcement authority. However, before filing a CCPA action, the California Attorney General must notify the offending business, service provider, or other person of the alleged violation and give them at least 30 days to cure it. If the company does not or cannot correct the violations, the Attorney General may seek civil penalties of up to $2,500 (US Dollar 2,500) per violation and $7,500 (US Dollar) per wilful violation.[170] The CCPA also provides for a private right of action for unauthorised access, theft, or disclosure of non-encrypted and un-redacted personal information.[171]

3.3.2.2 Colorado:

i. The Colorado Privacy Act,2023:

The Colorado Privacy Act, 2023 is a new law that takes effect on July 1, 2023. This law requires businesses to disclose their data collection and sharing practices to consumers and gives Colorado residents the right to opt out of the sale of their personal data. The broad definition of "personal data" under this Act includes any information linked or reasonably linkable to an indentified or indentifiable individual or natural person, the definition however excludes de-identified data or publicly available information.

The law also imposes strict penalties for companies and authorises the State Attorney General to bring enforcement actions for violations of the provisions

---

[170] California Consumer Privacy Act 2018, Section1798.155(b) states:- " *A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General".*

[171] Available at: https://www.csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html, (Last accessed on October 18,2021).

of this Act.[172]

3.3.2.3 Connecticut:

i. The Connecticut Personal Data Privacy and Online Monitoring Act, 2023:

The Connecticut Personal Data Privacy and Online Monitoring Act,2023 takes effect on July 1, 2023 and is intended to cover all business that collect personal information from Connecticut residents. It protects a Connecticut resident acting in an individual or household context, such as browsing the Internet or making a purchase at a store. It however does not protect an individual acting in an employment context, such as applying for a job. The law lays down privacy protection regulations for Data Controllers and Data Processors and requires them to take reasonable security measures to protect the personal data.[173]

The Act provides that entities or individuals may face civil penalties up to $5,000 (US Dollar 5,000) per violation, pursuant to the Connecticut Unfair Trade Practices Act and in addition to civil penalties the State Attorney General can also seek injunctive relief, restitution, and/or disgorgement.[174]

3.3.2.4 Maryland:

i. The Maryland Online Consumer Protection Act,2022:

The Maryland Online Consumer Protection Act,2022 protects consumers in Maryland from cybersecurity threats, including data breaches, theft, phishing, and spyware. While this law is similar to other State privacy laws, it's more comprehensive in certain respects, for instance, this law requires businesses to

---

[172] The Colorado Privacy Act,2023, available at; https://leg.colorado.gov/bills/sb21-190 (Last accessed on May 12,2023).

[173] The Connecticut Personal Data Privacy and Online Monitoring Act, 2023, available at: https://portal.ct.gov/AG/Sections/Privacy/The-Connecticut-Data-Privacy-Act (last accessed on May 12, 2023).

[174] Merriam-Webster Dictionary, Disgorgement means:- *remedy requiring a party who profits from illegal or wrongful acts to give up any profits they made as a result of that illegal or wrongful conduct. The purpose of this remedy is to prevent unjust enrichment and make illegal conduct unprofitable*, available at: https://www.merriam-webster.com/dictionary/disgorge (Last accessed on May 12, 2023).

take reasonable steps to protect consumers' personal information from unauthorised access, use, or disclosure. The law also requires entities to provide consumers with a way to opt out of having their personal information collected, used, or sold.

This Act applies to all businesses that collect, use, or disclose personal data about Maryland residents, including out-of-state companies that sell goods or services to Maryland locals.[175]

3.3.2.5 Massachusetts:

i. The Massachusetts Data Privacy Law, 2009:

In response to a surge in data breaches and global consumer data theft, the State of Massachusetts enacted a comprehensive data security legislation known as the *Massachusetts Data Privacy Law* in 2009.[176]

Based on this Act, the Massachusetts *Data Security Regulations 2010* were formulated, which require every company that owns or licenses "personal information" about Massachusetts residents to develop, implement, and maintain a comprehensive *Written Information Security Program* **("WISP").** The WISP must contain certain minimum administrative, technical, and physical safeguards to protect such "personal information".

In 2019, the law was updated and amended in response to new challenges in the digital and data worlds. As part of the new amendments, all entities must produce a WISP to confirm their compliance and in relation to an organisation's

---

[175] The Maryland Online Consumer Protection Act, 2022, available at: https://www.marylandattorneygeneral.gov/CPD%20Documents/Tips-Publications/Consumer_Guide_ to_ Protecting_Privacy.pdf (Last accessed on May 12, 2023).

[176] The Massachusetts Data Privacy Law, 2009, available at: https://www.mass.gov/info-details/massachusetts-law-about-privacy, (Last accessed on October 17, 2021).

IT systems, the WISP must include appropriate administrative, technical, and physical safeguards.

The compliance under this Act is not sector or industry specific, and it does not discriminate based on where an organisation is located. Any organisation that processes, stores, transmits, sells, or handles the information of Massachusetts residents is required to follow the State's data privacy laws. Noncompliance with the law currently entails fines of up to $5,000 (US Dollar 5,000) per violation, plus the reasonable cost of litigation and prosecution.

On February 2, 2022, a new draft of the *Massachusetts Information Privacy and Security Act* **("MIPSA")**, was released and is currently being considered for approval. This new version of the bill is envisaged to include new legislation that will have a significant impact on Massachusetts data privacy laws.[177]

3.3.2.6. New York:

i. The New York Privacy Act, 2021:

The New York Privacy Act, 2021 requires companies to disclose their methods for de-identifying personal data and to implement safeguards for personal data sharing. It also gives consumers the right to know the identities of the entities that have access to their data. Thus this Act gives New York consumers more control over their personal information and requires companies to manage personal data responsibly and legally and requires them to notify customers of; (a).consumer data rights, including the ability to withdraw consent (b).personal data categories processed by the company or any third-party entity (c). identification of all parties to whom the company discloses, shares, transfers, or sells personal information (d).the origin and goal of data collection and

---

[177] What is the Massachusetts Data Privacy Law (MIPSA)?, Available at: https://www.centraleyes.com/what-is-the-massachusetts-data-privacy-law-mipsa/#:~:text=The%20Massachusetts%20privacy%20act%20requires,a%20comprehensive%20information%20security%20program%E2%80%9D,(Last accessed on October 17, 2021).

processing (e).the period of retention for each type of personal data collected and processed (f).the use of personal data for targeted advertising, as well as the expected "average revenue per user" generated by targeted advertising.

The Act also requires companies to obtain unambiguous and informed opt-in consent from customers in order to allow the personal data processing. It also requires that the category and purpose for collecting and processing the data must be clearly described in the company's request for opt-in consent.

This Act applies to all legal entities that do business in New York or provide products or services to New York residents and meet the criteria of; (a). have a yearly gross revenue of at least $25 million (US Dollar 25 million) (b).control or process the personal data of 100,000 or more customers (c). control or process the personal data of 500,000 natural persons or more across the country, as well as 10,000 consumers and, (d). sell personal data and control or process the personal data of 25,000 or more consumers to generate more than 50% of gross revenue.

The Act provides that any violations of the provisions of this Act may result in a civil penalty of up to $15,000 (US Dollar 15,000), depending on the nature, severity, duration, wilfulness, and persistence of the misconduct. The law interestingly considers each unlawful processing of a consumer's personal data separately.[178]

3.3.2.7. Ohio:

i. Ohio Data Protection Act, 2018:

The State of Ohio enacted the *Data Protection Act,2018* which establishes an incentive-based programme to help companies improve their cyber security

[178] The New York Privacy Act, 2021,available at: https://www.bitraser.com/article/new-york-data-privacy-law.php, (Last accessed on October 17, 2021).

practises.

The Act in particular, provides companies with a safe harbour against data breach claims based on tort (such as negligence) brought under Ohio law or in Ohio courts for companies that implement, maintain, and comply with one of several industry recognised cyber security programmes. Significantly, however the Act expressly states that it does not create a minimum cyber security standard that must be achieved or impose liability upon companies that do not obtain or maintain practices in compliance with the Act. Rather, it aims to provide an incentive and encourage companies to achieve a higher level of cyber security through voluntary action.

To be eligible for the safe harbour, an entity must implement a written cyber security programme that: (a). protects the security and confidentiality of personal information (b). protects against anticipated threats or hazards to the security or integrity of personal information; and (c)protects against unauthorised access to and acquisition of personal information that is likely to result in a material risk of identity theft or fraud.[179]

The Act provides that to comply with the Act, an entity must create, maintain, and adhere to a written cyber security programme that includes administrative, technical, and physical safeguards to protect personal and/or restricted information and that reasonably conforms to an industry-recognised cyber security framework, ensures the security and confidentiality of personal and/or restricted data and guards against any potential threats or hazards to the security or integrity of personal and/or restricted data.

The Act also requires the entity's cyber security programme to "reasonably conform" to one of the following frameworks: (a).Cybersecurity Framework of

[179] The Ohio Data Protection Act, 2018**,** a**v**ailable at: https://kirkpatrickprice.com/blog/what-is-the-ohio-data-protection-act/, (Last accessed on October 18, 2021).

the National Institute of Standards and Technology ("NIST") (b).Security Assessment Framework of the Federal Risk and Authorization Management Program ("FedRAMP") (c).Critical Security Controls for effective Cyber Defense from the Center for Internet Security or (d). The ISO/IEC 27000 Information Security Management Systems Standards developed by the International Organisation for Standardisation ("ISO") and the International Electrotechnical Commission ("IEC").[180]

Thus this Act represents the first law in the US to provide incentives to entities to implement certain cybersecurity controls through the self affirmative defense to liability in the wake of a data breach.

3.3.2.8. Virginia:

i. Virginia Consumer Data Protection Act, 2021. ("VCDPA"):

Virginia has enacted a comprehensive data privacy legislation i.e. the *Virginia Consumer Data Protection Act, 2021* ("VCDPA"), which applies to companies that are not headquartered or incorporated in Virginia but do business there. It also applies to companies that, control or process the personal data of at least 100,000 Virginia residents, or control or process the personal data of at least 25,000 Virginia residents and derive more than 50% of their gross revenue from the sale of personal data.

The VCDPA gives consumers the following rights concerning their personal data guaranteed by the Act:

(a). the right to know about, access, and confirm personal information (b).the right to have personal data deleted, (b). the right to have inaccuracies in personal data corrected (c). data portability is made a legal right (i.e., easy,

---

[180] Ohio Bar, Practice Library Search, available at: https://www.ohiobar.org/member-tools-benefits/practice-resources/practice-library-search/practice-library/2019-ohio-lawyer/ohios-data-protection-act/#:~:text=Specifically%2C%20the%20DPA%20provides%20companies,several%20industry%2Drecognized%20cybersecurity%20programs (Last accessed on October 18, 2021).

portable access to all pieces of personal data held by a company) (e). the right to refuse the processing of personal data for the purposes of targeted advertising (f). the right to refuse the sale of personal information (g).the right to refuse profiling based on personal information (h).the right not to face discrimination for exercising any of the preceding rights.[181]

The Virginia Attorney General is empowered to enforce the VCDPA, which provides for a 30-day cure period to any violating company, but uncured non-compliance can result in a civil penalty of up to $7,500 (US Dollar 7,500) per violation.[182]

It thus appears that the United States has a patchwork and ever-changing web of laws governing data privacy and while there is no comprehensive federal privacy decree, several laws do focus on specific data types or situations regarding privacy.

The States and the respective Acts considered above are not comprehensive and apart from the statutes considered above, other States of the US may have their own data privacy laws which may have escaped mention, however considering the limitations of the present research, only the pertinent US State data protection laws are considered for the purpose of the present research.

3.4. DATA PROTECTION LAWS IN THE UNITED KINGDOM:

3.4.1. The Evolution of Data Protection in the United Kingdom:

The progression of data protection in the United Kingdom can be traced back to the 1970s. Several private members attempts to introduce legislation in the 1960s were unsuccessful, but the 1970s saw the publication of the Younger Report on Privacy

[181] Virginia Consumer Data Protection Act, 2021, available at; https://law.lis.virginia.gov/vacode/title59.1/chapter53/, (Last accessed on October 17, 2021).

[182] An overview of Virginia Consumer Data Protection Act, available at :https://www.hutchlaw.com/blog/an-overview-of-the-virginia-consumer-data-protection-act, (Last accessed on October 17, 2021).

(1972) and the Lindop Report on Data Protection (1974) & (1978). Both reports investigated the privacy risks posed by the increased use of computers to process personal information. It was however Sir Kenneth Younger[183], on the other hand, was the first to formulate the general principles of data protection, which now serve as the foundation for all data protection legislation.

3.4.2. The Council of Europe and the Organisation for Economic Cooperation and Development:

The publication of two international legal instruments on data protection in the early 1980's provided impetus for the government to introduce Data Protection legislation in the UK i.e. the *OECD Guidelines* in 1980 and the *Council of Europe Convention* in 1981.

The Council of Europe Convention makes it clear that its goal was to strike a balance between the need to allow for the movement of personal data and the need to protect personal privacy[184]. The *European Convention on Human Rights* and particularly Articles 8 and 10 thereof, served as the foundation for the Council of Europe Convention which recognised the need for a specific convention to address the risks posed by computer processing rather than relying solely on the general principles.

3.4.3. The Data Protection Act 1984:

The *Data Protection Act 1984* incorporated the general principles outlined in the Council of Europe Convention and the OECD Guidelines into a regulatory

---

[183] Sir Kenneth Gilmour Younger KBE (15 December 1908 – 19 May 1976) was a British Labour politician and barrister who served in junior government posts during the Attlee government and was an opposition spokesman under Hugh Gaitskell , available at: https://artsandculture.google.com/entity/kenneth-younger/m0dst4k?hl=en (Last accessed on October 18, 2021).

[184] What is Freedom of Information & Data Protection?, available at : https://www.ucl.ac.uk/constitution-unit/research/research-archive/foi-archive/what-freedom-information-data-protection#~:text= The%20development%20of%20Data%20Protection,to% 2Ddate%20 and%20lawfully%20used (Last accessed on October 18, 2021).

framework. At its heart was a public register of organisations in both the public and private sectors that processed personal data in the UK, which was overseen by an official known as the *Data Protection Registrar*, who was given enforcement powers. This Act established new rights for individuals in the UK, the most important of which were the right to know if an organisation was processing personal data about them and the right to a copy of that data (i.e. the right of subject access). Individuals under this Act could also file a complaint with the Data Protection Registrar.

However, the impact of the this Act was limited as it only applied to data stored on a computer, the enforcement regime was cumbersome and overly dependent on the Data Protection Registrar, and importantly Data Protection was not recognised as a privacy right. Nonetheless, the Data Protection Registrar and the Data Protection Tribunal formed under this Act, developed and established jurisprudence that positively impacted standards of personal data processing in the UK, particularly in interpreting the general principle of fairness to require transparency and a degree of control by data users.[185]

3.4.4. The European Union Directive, 1995 (Directive 95/46/EC):

The European Commission in 1990 published a draft directive, for pursuing the single market purpose and concerned that the free movement of data within the EU boundaries could be hampered due to widely dissimilar data protection standards across member states while some member states had no relevant legislation at all.
Thus, to address these issues, on October 24, 1995, the European Council formally approved the directive (i.e. Directive 95/46/EC).

[185] The Data Protection Act 1984,available at: https://www.ucl.ac.uk/constitution-unit/research/research-archive/foi-archive/what-freedom-information-data-protection#:~:text=The%20development%20of%20Data%20Protection,to%2Ddate%20and%20lawfully%20used (Last accessed on October 22, 2021).

The Directive proposed establishing relatively high data protection standards within the member States while ensuring that the level of protection already provided by existing national laws of the member States was not reduced.

While, the Directive was a mixture of broad general principles and detailed prescriptive measures, many of which only reflected the domestic interests of particular member States. The Directive however explicitly established the link between Data Protection and Personal Privacy.[186]

3.4.5. The Data Protection Act, 1998 ("DPA 1998") :

In pursuance to the recommendations made by the European Union Directive (Directive 95/46/EC), the Government of UK framed the *Data Protection Act of 1998* replacing the Data Protection Act of 1984, which now granted the UK individuals the rights to access to their personal data, challenge misuse of it, and seek redress. The Act, designated the *Information Commissioner* as the Authority in charge of enforcing the Act.

The Act provided for eight guiding principles for processing of individual personal data, which are as follows[187]:

---

[186] *Ibid* at 182.

[187] Data Protection Act 1998, Data Protection Principles, Schedule 1, Part 1 states:-

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
(a)at least one of the conditions in Schedule 2 is met, and
(b)in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Available at: https://www.legislation.gov.uk/ukpga/1998/29/schedule/1/enacted, (Last accessed on October 21, 2021).

i. **Principle of Just and Lawful processing:** This principle provided that the **i**ndividuals' personal data should be controlled and processed lawfully and fairly and included a *Fair Processing Notification*, which required the Data Controller to notify the individual of; (a).the data controller's identification (b).the intended purposes for which personal data will be processed and, (c). identity of who may have access to the individual's personal information.

ii. **The Objectives principle:** This principle mandates that the personal information of individual should only be obtained if it is intended to be used lawfully and should not be processed in any way that is incompatible with the intended purpose.

iii. **Principle of Sufficiency:** In terms of this principle, personal data processed should be adequate, relevant and not excessive in relation to the purpose for which it will be used.

iv. **Principle of Accurateness:** This principle provides that personal information should be accurate and up to date. When personal information becomes inaccurate, it should no longer be used for the intended purpose.

v. **Principle of Preservation:** In terms of this principle, personal data should not be kept for any longer than necessary for the purpose of processing. Personal information cannot be stored indefinitely.

vi. **Principle of Entitlement:** This principle provides that individuals' rights should be respected when processing personal data and mentions the following rights: (a)Access to personal data (b).Preventing processes that are likely to cause harm or distress (c).Restricting direct marketing (d).Creating automated decisions Correcting inaccurate personal data and, (e).Reimbursement.

vii. **Principle of Protection:** In terms of this principle, personal data should be safeguarded using reasonable and practical technical and organisational measures to preserve the integrity as well as individual's rights and freedoms against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to the personal data.

viii. **Principle regarding transfer of personal data:** In terms of this principle, personal data should not be transferred outside the EU unless the recipient country has sufficient data protection measures in place in order to protect data subject's i.e. individual's freedoms and rights regarding personal data.

The Act provides that any person or organisation that holds personal information about living individuals i.e. personal data (of UK citizens) on computer or in certain manual data systems, or has such information processed on computer by others is mandatorily required to comply with the Act's data protection principles and notify the Information Commissioner about the processing. The Act made the Data Controller (i.e. the person who controlled the purpose for which personal data was held and processed) responsible for ensuring compliance with the Act's Principles.[188]

Remedies for personal data misuse provided under this Act include compensation (if the individual has been harmed), rectification or destruction of inaccurate data, and the right to request a review by the Information Commissioner in matters of violation of the individual's data protection rights.

Incidentally, this Act was in effect until May 25, 2018, when it was superseded by the Data Protection Act 2018.

3.4.6. The Data Protection Act, 2018 ("UK GDPR"):

The United Kingdom left the European Union on December 31, 2021. Following Brexit, the UK is no longer subject to the EU GDPR, which governs the processing of personal data from individuals within the EU. Instead, the UK has its own version called the *Data Protection Act, 2018* **("UK GDPR")**.

---

[188] British Computer Society, Data Protection Act 1998 overview, Available at: https://www.bcs.org/articles-opinion-and-research/data-protection-act-1998-overview/ (Last accessed on October 22, 2021).

Interestingly, the UK GDPR is nearly identical to the EU GDPR in that, it requires the user website to obtain explicit consent from users before processing their personal data via cookies and third-party trackers, it requires organisations to safely store and document each valid user consent, it requires the user website to allow users to change their consent just as easily as they gave it, and it grants UK users a set of rights, chief among them is the right to delete and the right to be forgotten.[189]

It was necessitated because, following Brexit, the EU has designated the UK as a "*third country*" under the EU GDPR. However, on June 28, 2021, the EU adopted the "adequacy decision for the UK"[190], ensuring the continuation of free flow of personal data from individuals within the EU to the UK and vice-versa. Thus, personal data can now fluidly flow from the EU to the UK, where it is protected to an essentially equal level to that guaranteed by EU law by virtue of the UK GDPR., and it also aids in the proper implementation of the EU-UK Trade and Cooperation Agreement, which calls for the exchanging of personal information, such as for judicial cooperation.

Importantly, the UK adequacy decision of the EU is limited to four years and will not be automatically renewed, thus, in June 2025, a new adequacy process will be required to determine whether the UK still provides an equivalent level of data protection.

All of this means that there are still two GDPR's in effect in the UK, one applies if the organisation has users from the EU (i.e. the EU GDPR will be applicable), and the other if, if the organisation has users from the UK (i.e. the UK-GDPR will be applicable).

---

[189] UK Data Protection Act 2018, available at: https://www.cookiebot.com/en/data-protection-act-2018/ (Last accessed on July26, 2022).

[190] Commission implementing decision of 28.6.2021pursuant to regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183,(Last accessed on July 27, 2022).

It is important to note that the UK GDPR applies the same requirements for personal data processing to the *UK Intelligence Services* in the area of national security, which is outside the scope of the EU GDPR. It also gives the UK Home Office the authority to refuse personal data access requests based on the risk they may pose to immigration enforcement.

The UK GDPR provides that everyone in the UK who is in charge of using personal data must adhere to strict guidelines known as "data protection principles". Article 5 of the Act outlines seven key principles that emphasise the General Data Protection regime, and which are as follows[191] :

i. **The Principle of Lawfulness, Fairness, and Transparency:** This principle requires that personal data in relation to the data subject (i.e. the individual) must be processed lawfully, fairly, and transparently by; (a). identifying legal grounds for collecting or using personal data (b). ensuring that the data use does not violate any other laws, and (c). using data in a fair manner, i.e. not in a way that is detrimental, unforeseen, or misrepresenting to the individuals involved.

---

[191] Data Protection Act,2018, Article 5 states:- *Principles relating to processing of personal data:*
1.Personal data shall be:
(a)processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
(b)collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
(c)adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
(d)accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
(e)kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
(f)processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'), available at, https://www.legislation.gov.uk/eur/2016/679/article/5, (Last accessed on July 27, 2022).

Be straightforward, direct, and truthful with people about how you intend to use their personal data.

ii. **The Principle of Purpose Limitation:** This principle mandates that personal data must only be collected for a specific, explicit, and legitimate purpose.

iii. **The Principle of Data Minimization:** This principle requires that the personal data processed is: (a). sufficient to achieve the stated goal (b). has a logical connection to that purpose and, (c). is limited to what is required for that purpose.

iv. **The Principle of Accuracy:** According to this principle, all reasonable steps are required to be taken: (a). to make sure that the personal data held or processed is accurate and not misleading (b). that the origin and status of personal data is known (c). to carefully evaluate any challenges to information accuracy and, (d). to contemplate whether it is necessary to update the information on a regular basis.

v. **The Principle of Storage Limitation:** This principle requires that the personal data should not be stored for a period longer than necessary. Thus it requires the Data Processor to justify: (a). how long it intends to keep the data depending on the purpose for which it is required and, wherever feasible, set a retention period or timeframe to comply with the reporting requirements (b). review this data on a regular basis and delete or anonymise it when it is no longer required and, (c). challenges to data retention, such as erasure, should be carefully considered.

vi. **The Principle of Integrity and Confidentiality:** This principle requires that Data Processor must have appropriate security measures in place to protect the data it holds in order to comply with security requirements. This entails safeguarding the data: (a). against unlicensed or illegal processing (b).against unforeseen loss, destruction, or damage and, (c).implement appropriate technological or organisational measures.

vii. **The Principle of Accountability:** This principle requires the Data Processor to accept responsibility for how it handles personal data and how it adheres to the other principles by having appropriate measures and records in place.

The UK GDPR considers individuals whose personal data is being used, processed, or transferred as *"data subjects"* and confer certain rights upon them, which are as under:

i. **Right to Information :** This right entails giving individuals clear and concise information about how their personal data will be used. The Data Processor must provide the data subjects with specific privacy information about: (a).its company and business (b). Its purposes and legal grounds for processing the personal data (c).who the data will be shared with, including details of international transfers, and the retention periods for that personal data (d).the processing rights that are available to them, and (d) the capability to file a complaint based on the type of processing. [192]

ii. **Right of access to information *also known as* Subject Access Request :** Individuals have the right to access and obtain a copy of their personal data, as well as any additional information. This is commonly known as *Subject Access Request* **("SAR").** Individuals can submit SAR's either verbally or in writing, including through social media. A request is valid if it is clear that the individual is requesting their own personal information. A third party (such as a relative, friend, or solicitor) can also file a SAR on behalf of the individual subject to they providing proof of their authority to act on behalf of the data subject.

When a valid SAR is received, the Data Processor must conduct a thorough search for the requested information and respond within one month of receiving

---

[192] Data Protection Act 2018, Article 13 states:- *Information to be provided where personal data are collected from the data subject :*
1.Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
(a)the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d)where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of relevant adequacy regulations under section 17A of the 2018 Act, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
Available at : https://www.legislation.gov.uk/eur/2016/679/article/13,(Last accessed on July 27, 2022).

the request. In certain circumstances, the time limit may be extended by another two months. The information should be provided in a clear, concise, and understandable manner. Importantly the information should be disclosed also in a secure manner. Only if an exemption or restriction applies, or if the request is clearly unfounded or excessive, can the information be refused. In most cases, no fee is charged to handle a SAR request. [193]

iii. **Right of Correction or Rectification :** Individuals in the UK have the right to have their inaccurate personal data corrected or completed if it is insufficient. For this, a rectification request can be submitted either verbally or in writing. If such a request is received, the Data Processor must respond promptly and within one month of receipt, unless the time limit is extended and should take reasonable steps to ensure that the data is correct and, if necessary, correct it. [194]

iv. **Right to be forgotten / Right to Erasure :** Individuals have the right to request erasure of their personal data in certain circumstances, including the following: (a). where the Data Processor has illegally processed their data (b).the data is no longer required for the original purpose (c).where consent to process or store

---

[193] Data Protection Act,2018 , Article 15 states:- *Right of access by the data subject:*
1.The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
(a)the purposes of the processing;
(b)the categories of personal data concerned;
(c)the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
(*d)where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*
(e)the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f)the right to lodge a complaint with the Commissioner;
(g)where the personal data are not collected from the data subject, any available information as to their source;
(h)the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
Available at: https://www.legislation.gov.uk/eur/2016/679/article/15,(Last accessed on July 27,2022).

[194] Data Protection Act,2018, Article 16 states:- *Right to rectification:*
The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

data is withdrawn (d). they exercise their right to oppose to processing (e). Where erasure is required to comply with other legal obligations. [195]

v. **Right to restrict or limit processing:** Individuals can request limit on the processing of their personal data if: (a).they believe their data is inaccurate (b).although the processing is illegal, the individual does not want the data erased (c). The Data Processor longer requires the data, but the individual does in order to pursue a legal claim and, (d).The Data Processor is verifying overriding grounds in the context of a request.

In terms of the Act, where a request for restricting processing is made, the Data Processor will be able to store the data but not use it. Restriction requests can be made either verbally or in writing and response is required to be given within one month from the date of the request. Importantly, if a request for correcting, deleting, or limiting the processing of their data is made, the Data Processor must notify any third party with whom it has shared the data that the individual has exercised those rights. [196]

vi. **Right of Data Portability or Freedom to move Data :** Individuals have the right to receive a copy of their personal data for personal use and/or to have their

---

[195] Data Protection Act,2018, Article 17(1)states,*:- Right to erasure ('right to be forgotten')*
1.The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
(a)the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b)the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(c)the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d)the personal data have been unlawfully processed;
(e)the personal data have to be erased for compliance with a legal obligation ***[F1****under domestic law****];***
(f)the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

[196] Data Protection Act,2018, Article 18(1) states:- Right to restriction of processing:
1.The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
(a)the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
(b)the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
(c)the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
(d)the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

personal data transmitted from one controller to another. This right is only applicable when: (a).consent or contract is the legal basis for processing this information (b). the processing is carried out automatically, excluding paper files.[197]

vii. **Right of objection to processing:** Individuals have the right to object to the processing of their personal data in certain circumstances like that of direct marketing purposes. Individuals may also object if the processing is being done for: (a). a task in the public's interest (b). the exercise of official authority, or (c). legitimate concerns (or those of a third party).

This right to object is not absolute and the objection must be justified and may be expressed orally or in writing. [198]

viii. **Automated decision-making rights, including profiling:** Individuals have the right not to be subjected to a decision based on: (a). automated person decision making i.e. making a decision solely through automated means without any human involvement (b). profiling i.e. automated processing of personal data to determine certain aspects of an individual. [199]

---

[197] Data Protection Act,2018, Article 20(1) states:- *Right to data portability:*
1.The data subject shall have the right to receive the 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 have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
(a)the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
(b)the processing is carried out by automated means.

[198] Data Protection Act,2018, *Article 21 states, Right to object:*
1.The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
2.Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

[199] Data Protection Act,2018, Article 22(1) states:- *Automated individual decision-making, including profiling*
1.The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

3.4.6.1 Legal basis for Processing Personal Data under UK GDPR:

To process personal data in accordance with the UK GDPR, there must be a valid legal basis and the Act provides for six legal bases for processing of the personal data available and least one of these must be followed whenever personal data is processed.[200]

The following are legal bases for processing personal data:

i. **Consent:** This means that the individual has to expressly authorise the Data Processor to process their personal data for a specific purpose. Children under this Act require special safeguards when collecting and processing personal data because they may be less aware of the risks involved.

   When offering an online service directly to a child and relying on consent as the lawful basis for processing, only children aged 13 years or over can give their own consent in the UK. For children under this age, prior permission from the person who has parental responsibility for the child is required to be obtained.[201]

---

[200] Data Protection Act, 2018, Article 6(1) states:- *Lawfulness of processing:*
1.Processing shall be lawful only if and to the extent that at least one of the following applies:
(a)the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b)processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c)processing is necessary for compliance with a legal obligation to which the controller is subject;
(d)processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e)processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f)processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

[201] Data Protection Act,2018,Article 8(1) states:- *Conditions applicable to child's consent in relation to information society services*
1.Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

ii. **Contract:** This applies when processing is required to provide a contractual service to an individual or when they have requested to do something prior to entering into a contract (e.g. providing a quotation).

iii. **Legal compulsion:** This applies when processing is required to meet a common law or statutory obligation (not including contractual obligations). To rely on this ground, the Data processor must be able to identify either the specific legal provision or an appropriate source of advice or guidance that clearly defines its obligation.

iv. **Important considerations:** This applies when processing is required to save someone's life.

v. **Public duty:** This applies when processing is required to perform a task in the public interest or to carry out official duties, both of which have a clear legal basis.

   This is mostly applicable to public authorities in the UK, but it can apply to any establishment that exercises legitimate authority or performs public-interest tasks.

vi. **Genuine interest:** This applies when processing is required to satisfy the Data Processor's (or a third party's) legitimate interests. It is most likely to be appropriate when people's data is used in ways they would reasonably expect and with minimal privacy impact, or when there is a compelling justification for the processing.

   To rely on this ground, the Data Processor must first identify the interest, demonstrate that the processing is required to achieve it, and weigh it against the individual's interests, rights, and freedoms.

Thus, it can be understood that the majority of legal bases provided under the UK GDPR require that processing be *"necessary"* for a specific purpose. In this context, "necessary" means more than just useful or standard practise. It must be a targeted and proportionate method of accomplishing a specific goal. The Act requires that businesses must report a personal data breach if it is likely to jeopardise people's rights and freedoms, according to the UK GDPR.

3.4.6.2 Data breach under the UK GDPR :

The UK GDPR considers a personal data breach as any type of security incident, whether intentional or unintentional, that compromises the confidentiality, integrity, or availability of personal data of an individual[202]. For example, a breach is said to have could occurred: (a) if personal information is misplaced, destroyed, corrupted, or revealed (b). if someone gains access to or transmits personal data without proper authorisation or, (c). if the data is rendered inaccessible due to ransomware or accidental loss or damage and this inaccessibility has a significant negative impact on the individuals.

When such security-related incident occurs, Data Processor is required to determine as soon as possible whether a personal data breach has taken place.

The potential negative consequences for individuals should be the focus of this assessment and is required to be notified to the *UK Information Commissioner's Office* **("ICO")** and/or to the individuals affected by the breach.

---

[202] Data Protection Act,2018, Article 33 states:- *Notification of a personal data breach to the Commissioner:*
1.In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification under this paragraph is not made within 72 hours, it shall be accompanied by reasons for the delay.
2.The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3.The notification referred to in paragraph 1 shall at least:
(a)describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b)communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c)describe the likely consequences of the personal data breach;
(d)describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4.Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5.The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the Commissioner to verify compliance with this Article.

3.4.6.3 Penalties for violation of UK GDPR:

If a Data Processor fails to comply with the provisions of UK GDPR, the ICO under this Act is empowered to take enforcement action. For a violation of the regulation, the ICO may impose sanctions such as: (a). reprimands and warnings (b).order for compliance (c).impose restrictions on processing or data transfers (permanent or temporary) and, (d) impose administrative penalties.
The Act provides for these will actions to apply to both Data Controllers and Data Processors and may have a significant impact on the day-to-day operations of the business.

The Act further provides that failure to comply with the UK GDPR may result in significant fines which are divided into two categories: (a) for violations of provisions, such as legislative or administrative requirements, a maximum fine of £8.7 million (GBP 8.7 million) or 2% of annual global turnover of the organisation, whichever is greater can be imposed (b). for any violation of any of the data protection principles or individual rights, a maximum fine of £17.5 million (GBP 17.5 million) or 4% of annual global turnover of the organisation, whichever is greater can be imposed. [203]

---

[203] Data Protection Act,2018, Article 83(4) states:- *General conditions for imposing administrative fines :*
4.Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to £8,700,000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
(a)the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
(b)the obligations of the certification body pursuant to Articles 42 and 43;
(c)the obligations of the monitoring body pursuant to Article 41(4).
5.Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to £17,500,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
(a)the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
(b)the data subjects' rights pursuant to Articles 12 to 22;
(c)the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
(d)any obligations under Part 5 or 6 of Schedule 2 to the 2018 Act or regulations made under section 16(1)(c)
of the 2018 Act;
(e)non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the Commissioner pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

The Act however makes these fines optional rather than mandatory and they are to be imposed proportionately, on a case-by-case basis, and usually as a last resort by the ICO, and when determining the level of penalties, the ICO has to take into account a number of factors, including: (a).the nature, gravity, and duration of the violation (b).the number of people affected and the extent of their injuries (c).whether the violation was intentional or unintentional (c).any prior record of noncompliance (d).any action taken to lessen the damage and, (e).whether the controller reported the violation to the ICO and co-operated with the ICO is addressing the breach.

3.4.6.4 Statutory Independence of the Adjudicating Authority under the UK GDPR:

An important facet of the UK GDPR is the provision for the complete independence of the ICO,[204] who is designated as the UK's Independent Authority to protect information rights in the public interest by encouraging openness by public bodies and data privacy for individuals. The ICO is expected to be free of external influence, whether direct or indirect, and to not seek or accept instructions from anyone.[205]

Although the UK GDPR reduces the total number of principles from eight to six, the revamped regulation is much broader in scope than the previous legislations on data protection in the UK, giving individuals significantly larger control over their personal data and enforcing strict penalties on organisations that do not comply. It is

---

[204] Data Protection Act,2018, Article 52 states:- *Independence :*
1.The Commissioner shall act with complete independence in performing tasks and exercising powers in accordance with this Regulation.
2.The Commissioner shall, in the performance of tasks and exercise of powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
3.The Commissioner shall refrain from any action incompatible with the Commissioner's duties and shall not, while holding office, engage in any incompatible occupation, whether gainful or not.

[205] Lawful basis for processing of personal data, available at: https://www.nibusinessinfo.co.uk /content/lawful-basis-processing-personal-data, (Last accessed on July 28, 2022).

also worth noting that the laws apply to any entity or person that collects data on UK citizens, regardless of location.

Thus, to conclude, in this chapter, the existing legal framework and the various relevant provisions of the respective Data Protection Laws in Europe, United States of America including the diverse Federal and State laws therein and in the United Kingdom has been discussed in detail.

It is important to comprehend these laws and the constructive aspects and shortcoming's as India is at the cusp of framing it's own Personal Data Protection Law and it would benefit from adopting a forward-thinking approach as even digital trade is inextricably linked to the exchange of information, and hence a regime for data transfers along with protection of personal information is crucial and would afford an opportunity for India to adopt a suitable approach at the international level, thereby building mutually compatible legal approaches in this area.

In the ensuing chapter, the Researcher has highlighted the evolution of the Right to Life and Personal Liberty which now includes the Right to Privacy under Article 21 of the Indian Constitution and the present scenario of the existing Data Protection Laws prevalent in India. These legislations have been analysed in brief with special reference to the existing personal data privacy regulatory provisions.

CHAPTER 4 - EXISTING DATA PROTECTION LAWS IN INDIA: PRESENT SCENARIO.

4.1 INTRODUCTION:

The world is becoming more and more digitalised with each passing day, and India is no exception. With billions of people communicating with one another through the transmission of information via digital mediums, a massive amount of data is generated all over the world. The newly discovered digital mediums of information exchange, including social media intermediaries such as, *WhatsApp*, *Facebook*, *Instagram*, *Twitter*, and such other platforms, have a wide reach among a large portion of the population.

In India, the number of active Internet users is expected to increase by 45% in the next two years, reaching 900 million by 2025, up from around 622 million in 2020, thanks to the availability of cheaper internet and broader connectivity[202]. As a result, the digital ecosystem in the country will need to evolve to meet the unique needs of this emerging demographic. Over the next few years, voice, and video will emerge as game changers for the digital ecosystem. Furthermore, online payment *applications* **("Apps")** such as; *Swiggy*, *Zomato*, *Uber*, *Ola*, *Paytm* and *Google Pay* etc, already have created a strong presence in the Indian economy and the use of these Apps by citizens has contributed to the massive amount of personal data being generated in the digital sphere.

However, while these Apps do make it easier for users, providing safe storage of individual's personal data poses a significant threat to informational privacy and the unrestrained increasing use of the internet has raised a slew of concerns about the

[202] India to have 900 million actice internet users by 2025, Economic Times, available at: https://economictimes.indiatimes.com/tech/technology/india-to-have-900-million-active-internet-users-by-2025-says-report/articleshow/83200683.cms?from=mdr, (Last accessed on October 21 2022).

possibility of data breaches. With the Government being the largest processor of personal data in India, it is imperative to have a law in place that regulates the entire process of data collection, storage, and processing, as well as putting in place necessary safeguards. However, the danger to informational privacy in India, as well as the rest of the world, is not new, rather the threat has grown much larger with the advent of digitalisation.

Data protection thus entails a set of privacy legislation, policies, and procedures designed to limit the invasion of one's privacy generated by the collection, storage, and dissemination of personal data.

Existing laws and policies in India are primarily sectoral in nature. In addition to other sectoral legislations, the relevant provisions of the Information Technology Act, 2000 and the rules stipulated thereunder currently govern the collection, processing, and use of “personal information” and “sensitive personal data or information” by a corporate body in India.

In this chapter, the Researcher has critically analysed the the progression of the Right to Privacy in India enshrined under Article 21 of the Indian Constitution which is the cornerstone of data privacy, and the present situation of the existing Data Protection Laws in India while also presenting some of the reported instances of personal data violations in India .

4.2 JUDICIAL DEVELOPMENTS IN INDIA REGARDING THE RIGHT TO PRIVACY :

Unlike the EU, India does not have any separate law which is designed exclusively for the data protection. However, the courts on numeral instances have interpreted "*Data Protection*" within the ambits of *"Right to Privacy"* as implicit in Article 21 of the Constitution of India.

Article 21 of the Indian Constitution states that "*no person shall be deprived of his life or personal liberty except in accordance with the procedure established by law*".[203] However, the Indian Constitution does not explicitly recognise the "right to privacy" as a fundamental right.

The Hon'ble Supreme Court first considered whether the *"Right to Privacy"* is a fundamental right in the case of ***M. P. Sharma and Ors v Satish Chandra, District Magistrate, Delhi and Ors***,[204] in which the warrant issued for search and seizure under Sections 94 and 96 (1) of the Code of Criminal Procedure was challenged. The Supreme Court ruled that the power of search and seizure did not violate any constitutional provisions. Furthermore, the Hon'ble Supreme Court declined to recognise the right to privacy as a fundamental right guaranteed by the Indian Constitution.

Subsequently, in the case of ***Kharak Singh v State of Uttar Pradesh and Ors***,[205] the Hon'ble Supreme Court considered whether surveillance by domiciliary trips at night against such an accused would be a misuse of the constitutional right under Article 21 of the Indian Constitution, raising the question of whether Article 21 was inclusive of the right to privacy. The Supreme Court ruled that any such surveillance was in fact a violation of Article 21. The majority judges went on to say that because Article 21 does not expressly provide for a privacy provision, the right to privacy cannot be construed as a fundamental right.

In the case of ***Gobind v State of M.P.***[206] the police's right to conduct domiciliary surveillance was called into question as being incompatible with the right to privacy guaranteed by Article 21 of the Indian Constitution. The Supreme Court ruled that the police regulations were not in accordance with the core of personal freedom. It also recognised the right to privacy as a fundamental right guaranteed by the Indian

[203] The Constitution of India 1950, Article 21 states:- *Protection of life and personal liberty.—No person shall be deprived of his life or personal liberty except according to procedure established by law.*
[204] M. P. Sharma and Ors v. Satish Chandra, District Magistrate, Delhi and Ors 1954 SCR 1077.
[205] Kharak Singh v. State of Uttar Pradesh and Ors (1964) 1 SCR 334.
[206] Gobind v. State of M.P. (1975) 2 SCC 148.

Constitution, but favoured progression of the right to privacy on a case-by-case basis and rejected it as absolute in nature.

The Supreme Court held that privacy facilitates freedom and is intrinsic to the exercise of liberty, and instances of freedoms established in Articles 25, 26, and 28(3) of the Indian Constitution were provided to demonstrate how the right to privacy was required to exercise all of the aforementioned rights and the approach of categorising the freedoms granted under Part III of the Indian Constitution was rejected. Rather, it was held that such rights overlap and that limiting one freedom impacts the other, as previously held in the ***Maneka Gandhi v Union of India***,[207] and ***Rustom Cavasji Cooper v Union of India***[208] judgments. As a result, a law that restricts a freedom under Article 21 of the Indian Constitution would also have to meet the reasonableness requirements under Articles 19 and 14 of the Indian Constitution.

The Hon'ble Supreme Court affirmed a similar proposition in the case of ***R. Rajagopal and Anr. v State of Tamil Nadu,***[209]where it was observed that the right to privacy is implicit in the right to life and liberty guaranteed to citizens of this country by Article 21. It's a "right to be left alone." A citizen has the right to privacy regarding his or her own, family, marriage, procreation, motherhood, child-bearing, and education, among other things. Nobody can publish anything about the aforementioned subjects without his permission, whether true or false, effusive or critical. If he does so, he is violating the person's right to privacy and could face legal consequences. However, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy, the position may be different.

[207] Maneka Gandhi v. Union of India (1978) 1 SCC 248 .
[208] Rustom Cavasji Cooper v. Union of India (1970) 1 SCC 248.
[209] R. Rajagopal and Anr v. State of Tamil Nadu (1994) 6 SCC 632.

Following that, in ***People's Union for Civil Liberties (PUCL) v Union of India,***[210] The Supreme Court stated unequivocally that it had no hesitation in holding that right to privacy is a part of the right to "life" and "personal liberty" enshrined in Article 21 of the Constitution. It held that Article 21 is invoked when the facts of a given case constitute a right to privacy and this right cannot be limited “except in accordance with the procedure established by law”.

This issue was raised before the Hon'ble Supreme Court yet again in the case of ***K. S. Puttaswamy (Retd.) v Union of India,***[211] in which the “*Aadhaar Card Scheme*” was called into question on the grounds that obtaining and compiling biometric and demographic data of the residents of a country for different purposes violates the fundamental privacy right embodied in Article 21 of the Indian Constitution.

The Hon'ble Supreme Court held that the right to privacy is intrinsic to and inseparable from the human element in human beings and the core of human dignity while analysing the nature of the right to privacy in terms of its origin. As a result, it was decided that privacy has both positive and negative aspects. The negative content prevents the state from infringing on a citizen's life and personal liberty, while the positive content requires the state to take all necessary measures to protect the individual's privacy. As a result, the constitutional protection of privacy may give rise to two interconnected protections: (i) against the world as a whole to be treated with respect by all, including the State: the right to choose what private information is to be released into the public space; and (ii) against the State, as a necessary concomitant of democratic principles, limited government, and state power limitations.

As a result of this decision, the Right to Privacy has become more than a scant common law right and stronger and more sacrosanct than any statutory right. Thus,

[210] People's Union for Civil Liberties (PUCL) v. Union of India (1997) 1 SCC 301.
[211] *Supra* note 2 at 1.

in the context of Article 21 of the Constitution, an invasion of privacy must now be justified on the basis of "a law" that specifies a fair, just, and reasonable procedure.
In ***Navtej Singh Johar v Union of India,***[212] the Supreme Court unanimously ruled that Section 377 of the IPC, 1860, which criminalised carnal intercourse against the order of nature, was unconstitutional in the way it criminalised sexual conduct between two consenting adults. The court relied on its decision in the *Puttaswamy*[213] case when reasoning that discrimination on the basis of sexual orientation was a violation of the right to equality, that incarceration of consensual sex between adults in private was a violation of the right to privacy, that sexual preference is an inherent part of self-identity and that attempting to deny it would be a violation of the right to life, and that fundamental freedoms cannot be refused on the basis that they are incompatible with other rights.

In ***Vinit Kumar v CBI,***[214] the Bombay High Court viewed the interception of a businessman's phone calls through the lens of infringing on his right to privacy. The matter of this case was the Union Home Ministry ordering the interception of the said person's communications due to allegations of public servant bribery. The orders were contested, and the court ruled that there was no legal basis for them and overturned them. It heavily relied on the *Puttaswamy*[215] decision while also claiming that the Government did not follow the legislative requirements and procedure outlined in Section 5(2) and Rule 419A of the Telegraph Act.

In ***Subhranshu Rout @ Gugul v State Of Odisha,***[216] right to be forgotten was recognised by the High Court of Orissa as a subset of the right to privacy. During a bail hearing, the court mentioned how the right to be forgotten is a component of the right to privacy. It emphasised the importance of establishing frameworks to ensure that individuals can protect their privacy by exercising this right.

---

[212] Navtej Singh Johar v. Union of India (2018) 10 SCC 1.
[213] *Ibid* at 211.
[214] Vinit Kumar v. CBI,Writ Petition No. 2367 of 2019.
[215] *Id* at 211.
[216] Subhranshu Rout @ Gugul v. State Of Odisha BLAPL No.4592 OF 2020.

In ***Kush Kalra v Union of India***[217]**,** the Supreme Court ruled in this case that posting posters outside the homes of COVID positive patients is not permitted. This was because it violated fundamental rights such as the right to privacy and the right to live a dignified life. It was determined that the affixation of posters violated the right to privacy secured under article 21 of the Indian Constitution, as reaffirmed by the Supreme Court of India in the case of *Puttaswamy.*[218]

Thus, vide the *Puttaswamy*[219] judgment the Supreme Court established three requirements for the Government's interference with an individual's fundamental rights. While the Government may intervene to protect legitimate state interests: (a) there must be a law in place to justify an encroachment on privacy, which is an express requirement of Article 21 of the Constitution, (b) the nature and content of the law that imposes the restriction must fall only within zone of reasonableness required by Article 14, and (c) the means implemented by the legislature must be directly proportionate to the object and needs sought to be accomplished by the legislature. As a result, in the future, any laws that seek to infringe on an individual's right to privacy must pass through these parameters known as the "*proportionality test"*.

It will however take a few years for the jurisprudence on what constitutes reasonable and proportionate Government intervention to settle, however the decision of the Hon'ble Supreme Court in the *Puttaswamy*[220] case empowers Indian citizens to now seek judicial relief in the event of a violation of their data privacy rights.

[217] Kush Kalra v. Union of India Writ Petition (Civil) No.1213 Of 2020.
[218] *Ibid* at 211.
[219] *Id*.
[220] *Id*.

4.3 LEGISLATIVE DEVELOPMENTS FOR SECURING INFORMATION PRIVACY IN INDIA :

Personal data safety is intrinsically tied with privacy i.e. each person's right to enjoy his or her liberty and life without arbitrary interference with his or her personal life, family, home, or correspondence, among other things. The word “private” must be interpreted in contrast to the word “public”, and as a result, the right to be left alone and its protection are critical in today's intrusive information technology age. Since presently there is no single enactment in India that governs data protection comprehensively, the legal provisions governing the same are required to be derived from a variety of legislative enactments.

Presently, the main legislations dealing with data protection in India is the *Information Technology Act, 2000* **(“IT Act”)**, *the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009* **(“IT Rules, 2009”)** and *the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011* **(“SPDI Rules”)**, whereby “personal information” and “sensitive personal data or information” is primarily sought to be protected under the said IT Act, IT Rules, 2009 and the SPDI Rules.

Interestingly however, information that is freely available in the public domain is not considered “sensitive personal data or information” under these legislations and furthermore, the provisions only cover the gathering and dissemination of information by a “body corporate” and excludes Government and its agencies.

Thus, it is imperative to understand the various sectoral legislations which presently deal with data protection in India, which are as highlighted as follows:

4.3.1 The Information Technology Act, 2000 (as amended by the Information Technology Amendment Act, 2008) ("IT Act") :

The Information Technology Act, 2000 **("IT ACT")** was based on the United Nations Commission on International Trade Law's *Model Law on Electronic Commerce* and as such it appears to limit its scope to e-commerce activities, and the primary goal as can be envisaged from the definition of data under this Act, was to advance the cause of internet governance in the information technology sector as the IT Act uses a conventional e-commerce-oriented definition of the term "data".[221]

The emphasis on computer and other forms of memory storage contemplated under this Act, suggests the provision's original legislative intent. It should also be noted that the restricted meaning of the term data has undergone significant changes as a result of subsequent provisions dealing with the issues of compensation payment and punitive measures in cases of unlawful disclosure and misuse of personal data, as well as breach of contractual arrangements relating to personal data.

According to the IT Act, a body corporate that possesses, deals with, or handles any personal data or information and is negligent in implementing and maintaining reasonable security practises, resulting in wrongful loss or wrongful gain to any individual, may be held liable to pay for the damages to the person so afflicted. It is crucial to note that it excludes Government and its agencies, who may be engaged collecting or storing personal data and further no upper limit has been specified under this Act for the amount of compensation that can be claimed by the afflicted party in such circumstances.

---

[221] Information Technology Act, 2000, Section 2(o) states:- *'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnet ic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer*

Following amendments in 2008, the IT Act now includes numerous provisions for data protection, mandatory privacy policies, and penalties for violations of such privacy policies, though in a limited manner.

The following are the relevant IT Act provisions:

i. **Sections 43 (a), (b), and (i)** – provides for a liability of paying damages to the tune of Rs.1,00,00,000/- (Rupees One Crore) to the person who has been harmed by a person who accesses or obtains access to a computer, computer system, or computer network without the permission of the owner or any other person who may be in charge of such computer, computer system, or computer network, downloads, copies, or extracts any data, computer data base, or information from such computer, computer system, or computer network, including any information or data retained or stored on any removable storage medium, tries to steal, conceals, destroys, or modifies, or causes another person to steal, conceal, destroy, or modifies any computer source code used for a computer resource with the intent to cause damage.[222]
ii. **Section 43A -** This section is the cornerstone of IT Act and provides that if a body corporate is negligent in implementing and maintaining reasonable security practises and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages in the form of compensation of Rs.5,00,00,000/- (Rupees Five Crore).[223]

---

[222] Information Technology Act, 2000, Section 43 states:- *Penalty and Compensation for damage to computer, computer system, etc* -
If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network -
(a) accesses or secures access to such computer, computer system or computer network or computer resource
(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
See also: Information Technology Act, 2000, Section 43(i) states:-
(i) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

[223] Information Technology Act, 2000, Section 43A states:- *Compensation for failure to protect data* -
Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any

iii. **Section 66 C -** This section deals with identity theft and states that anyone who fraudulently or disingenuously uses another person's electronic signature, password, or some other unique identifying feature shall face imprisonment for a term of up to three years and a fine of up to Rs. 1,00,000/- (Rupees One Lakh).[224]

iv. **Section 66 E -** This section provides for anyone who intentionally or knowingly captures, publishes, or transmits an image of a private area of another person without his or her consent, in circumstances that violate that person's privacy, faces imprisonment for up to three years or a fine of not more than Rs.2,00,000/- (Rupees Two Lakh), or both.[225]

v. **Section 72 -** This section provides for any person who obtains access to any electronic record, book, register, correspondence, information, document, or other material without the consent of the person concerned and then discloses

---

person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected.
Explanation: For the purposes of this section
(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals
engaged in commercial or professional activities
(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.
(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

[224] Information Technology Act, 2000, Section 66C states:- *Punishment for identity theft -*
Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

[225] Information Technology Act, 2000, Section 66E states:- *Punishment for violation of privacy -*
Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both
Explanation.- For the purposes of this section—
(a) ―transmit‖ means to electronically send a visual image with the intent that it be viewed by a person or persons;
(b) ―capture‖, with respect to an image, means to videotape, photograph, film or record by any means;
(c) ―private area‖ means the naked or undergarment clad genitals, pubic area, buttocks or female breast;
(d) ―publishes‖ means reproduction in the printed or electronic form and making it available for public;
(e) ―under circumstances violating privacy‖ means circumstances in which a person can have a reasonable expectation that—
(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

such electronic record, book, register, correspondence, information, document, or other material to any other person shall be punished with imprisonment for a term of up to two years or a fine of up to Rs. 1,00,000/- (Indian Rupees One Lakh) or both.[226]

vi. **Section 72A –** In terms of this provision, any person, including an intermediary, who discloses, without the consent of the person concerned or in breach of a lawful contract, any material containing personal information about another person while providing services under the terms of a lawful contract, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain. shall be punished with imprisonment for a term which may extend up to three years, or with a fine which may extend up to Rs. 5,00,000 (Rupees Five Lakh), or both.[227]

Interestingly, the Act also provides for the grounds for Government interference with personal data if satisfied that doing so is necessary or expedient in the interest of India's sovereignty or integrity, defence of India, state security, and friendly relations with foreign countries States or public order, or to prevent incitement to violence, commission of any cognizable offence committed relating to the preceding or investigation of any offence, for reasons to be recorded in writing can direct any government agency to intercept, monitor, or decrypt or cause any

---

[226] Information Technology Act, 2000, Section 72 states:- *Breach of confidentiality and privacy -*
Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

[227] Information Technology Act, 2000, Section 72A states:- *Punishment for Disclosure of information in breach of lawful contract -*
Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

information generated, transmitted, received, or stored in any computer resource for reasons that must be documented in writing.[228]

4.3.2 Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ("IT Rules, 2009") :

The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 **("IT Rules, 2009")** have been notified in accordance with IT Act, and Rule 3 of the IT Rules, 2009 is a detailed provision that requires decryption, monitoring, or interception of any information to be done only with an order issued by a competent authority. In unavoidable circumstances, however, even a Government officer with the rank of Joint Secretary or higher can issue such an order. Interestingly the phrase "unavoidable circumstances" has no definition provided in these Rules.

It further provides that in an emergency, where prior instructions are not possible, or for operational reasons, interception, monitoring, or decryption may be carried out with the approval of the second most senior officer or the head of the security and law enforcement agency at the Central level. Such officers, however, cannot be lower in rank than the Inspector General of Police or an officer of equivalent rank at the State Government or Union Territory level and the officer who approved the interception or decryption is required to notify the competent authority in writing of such approvals.[229]

---

[228] Information Technology Act, 2000, Section 69 states:- *Powers to issue directions for interception or monitoring or decryption of any information through any computer resource* -
(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

[229] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, Rule 3 states:- *Direction for interception or monitoring or decryption of any information-*

While the IT Rules, 2009 establish the procedural safeguards that the Competent Authority must follow, they fall short of adequately protecting the rights of those who are monitored and do not qualify the proportionality, adequacy, and necessity test and thus face the following difficulties:

i. **Inadequate judicial oversight, resulting in a conflict of interest:** The Competent Authority and Review Committee envisaged under these Rules only include members of the executive. The orders for decryption are issued by the Competent Authority, and the Review Committee certifies the legality of these orders. As orders are issued and reviewed by the executive, this creates a conflict of interest. The element of judicial scrutiny used to ensure that the orders are issued and reviewed by the executive is ironically found missing from these Rules.

ii. **Opacity behind the procedures used:** The current framework envisaged under these Rules allows for and facilitates opacity behind the procedures used as well as the number of decryption orders issued each year, thus resulting in there being no data on India's surveillance framework. There is no way of knowing whether the Review Committee meets in the stipulated period of every two months or not,

---

No person shall carry out the interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource under sub-section (2) of section 69 of the Act, except by an order issued by the competent authority;
Provided that in an unavoidable circumstances, such order may be issued by an officer, not below the rank of Joint Secretary of the Government of India, who has been duly authorised by the competent authority;
Provided further that in a case of emergency–
(i) in remote areas, where obtaining of prior directions for interception or monitoring or decryption of information is not feasible; or
(ii) for operational reasons, where obtaining of prior directions for interception or monitoring or decryption of any information generation, transmitted, received or stored in any computer resource is not feasible, the interception or monitoring of decryption of any information generated, transmitted, received or stored in any computer resource may be carried out with the prior approval of the Head or the second senior most officer of the security and law enforcement agency (hereinafter referred to as the said security agency) at the Central level and the officer authorised in this behalf, not below the rank of the inspector General of Police or an officer of equivalent rank, at the State or Union territory level;
Provided also that the officer, who approved such interception or monitoring or decryption of information in case of emergency, shall inform in writing to the competent authority about the emergency and of such interception or monitoring or decryption within three working days and obtain the approval of the competent authority thereon within a period of seven working days and if the approval of competent authority is not obtained within the said period of seven working days, such interception or monitoring or decryption shall cease and the information shall not be intercepted or monitored or decrypted thereafter without the prior approval of the competent authority.

or whether it actually considers any orders issued by the Competent Authority to be in violation of the Rules.

iii. **Destruction of records of interception, monitoring, or information decryption:** The Rules require the destruction of records within the stipulated time period of 180 days or 6 months after the order is issued. This results in the denial of information regarding the number of such decryption orders that have been passed. It also means that if an aggrieved party discovers that he or she has been surveilled by law enforcement agencies, they have no way of proving in court that their right to privacy and anonymity was violated.[230]

Thus it can be inferred that the IT Rules, 2009 though provide for lawful interception and monitoring by Government agencies, it is opaque in safeguarding the right to privacy of the affected individuals.

4.3.3 The Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") :

Section 43A of the IT Act was invoked to issue the *Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011***("SPDI Rules")** and it deals with "compensation for failure to protect data" and allows for the implementation of "reasonable security practises and procedures" to protect *sensitive personal data.*[231] To a limited extent, the SPDI Rules

---

[230] Software Freedom Law Center, India, Section 69 of the Information Technology Act and Decryption, available at: https://sflc.in/s-69-information-technology-act-and-decryption-rules-absence-adequate-procedural-safeguards#sdfootnote3anc (Last accessed on October 27,2021).

[231] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Rule 3 states:- *Sensitive personal data or information of a person means such personal information which consists of information relating to;—*
(i) password;
(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history;
(vi) Biometric information;
(vii) any detail relating to the above clauses as provided to body corporate for providing service; and
(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

incorporate the OECD Guidelines specifically, collection limitation, purpose specification, use limitation, and individual participation. The SPDI Rules also impose certain requirements for information collection[232], and mandates that it be done only for a lawful purpose related to the organisation's function.[233]

Furthermore, in terms of these Rules every organisation is required to have a comprehensive privacy policy.[234] The SPDI Rules also specify how long information can be kept[235] and give individuals the right to have their information corrected[236] and disclosure is not permitted without the consent of the individual unless contractually permitted or required for legal compliance.[237]

---

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

[232] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Rule 5(1) states:-
Body corporate or any person on its behalf shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

[233] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Rule 5(2) states :-
Body corporate or any person on its behalf shall not collect sensitive personal data or information unless;
(a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and
(b) the collection of the sensitive personal data or information is considered necessary for that purpose.

[234] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011Rule 4 states:-
The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall be published on website of body corporate or any person on its behalf and shall provide for;
(i) Clear and easily accessible statements of its practices and policies;
(ii) type of personal or sensitive personal data or information collected under rule 3;
(iii) purpose of collection and usage of such information;
(iv) disclosure of information including sensitive personal data or information as provided in rule 6;
(v) reasonable security practices and procedures as provided under rule 8.

[235] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011,Rule 5(4) states:-
Body corporate or any person on its behalf holding sensitive personal data or information shall 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 other law for the time being in force.

[236] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011Rule 5(6) states:-
Body corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible:

Interestingly, in terms of these Rules, when it comes to sharing information with Government agencies, the individual's consent is not required, and such information can be shared for reasons such as identity verification, preventative measures, detection, and investigation of events, including cybersecurity incidents, prosecution, and punishment of offences.[238]

Incidentally the SPDI Rules applies only to corporate entities, leaving the Government and Government bodies and agencies out of its purview, the rules are limited to "sensitive personal data", which encompasses attributes such as sexual orientation, health records and history, biometric data, and so on[239], rather than the broader category of "personal data".

Provided that a body corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of information to such boy corporate or any other person acting on behalf of such body corporate.

[237] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Rule 6(1) states:-
Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation: Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

[238] *Ibid* at 237.

[239] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Rule 3 states:-
Sensitive personal data or information of a person means such personal information which consists of information relating to;—
(i) password;
(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history;
(vi) Biometric information;
(vii) any detail relating to the above clauses as provided to body corporate for providing service; and
(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:
provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

Furthermore, the *Cyber Appellate Tribunal* **("CyAT"),** which is provided as the Appellate forum under the IT Act which adjudicates on IT Act appeals, gave its last order in 2011.

Thus, the lack of an effective enforcement mechanism raises concerns about the SPDI Rules' implementation and therefore to adequately protect personal data in all of its dimensions, a comprehensive law must be enacted containing an effective enforcement mechanism.

4.3.4 The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act") :

The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services), 2016 (**"Aadhaar Act")** as this Act is generally known, empowers the Government to collect identifying information from citizens,[240] including biometrics, issue a unique identification number or an "Aadhaar Number" based on such biometric information,[241] and then deliver targeted subsidies, benefits, and services to them.[242]

---

[240] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 30 states:- *The biometric information collected and stored in electronic form, in accordance with this Act and regulations made thereunder, shall be deemed to be "electronic record" and "sensitive personal data or information", and the provisions contained in the Information Technology Act, 2000 and the rules made thereunder shall apply to such information, in addition to, and to the extent not in derogation of the provisions of this Act.*
Explanation.— For the purposes of this section, the expressions—
(a) "electronic form" shall have the same meaning as assigned to it in clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000;
(b) "electronic record" shall have the same meaning as assigned to it in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000;
(c) "sensitive personal data or information" shall have the same meaning as assigned to it in clause (iii) of the Explanation to section 43A of the Information Technology Act, 2000.

[241] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 3(1) states:- *Every resident shall be entitled to obtain an Aadhaar number by submitting his demographic information and biometric information by undergoing the process of enrolment: Provided that the Central Government may, from time to time, notify such other category of individuals who may be entitled to obtain an Aadhaar number.*

[242] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 7 states:- *The Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of, the Consolidated Fund of India, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual*

The Aadhaar Act also includes provisions for Aadhaar based authentication services, in which a requesting entity (Government/public and private entities/agencies) can ask the designated governing body i.e *Unique Identification Authority of India* **("UIDAI")** to verify/validate the accuracy of the identity information disclosed by individuals in order to provide services to them[243]. The Act provides that soliciting entity must obtain the individual's consent before obtaining the identity information for the purpose of authentication and may only use the identity information for the sole purpose of authentication.[244]

The Aadhaar Act establishes a governing body, i.e. the UIDAI, to oversee the implementation of the Act.[245] It also creates a *Central Identities Data Repository* **("CIDR")**[246], which is a database that holds Aadhaar Numbers as well as corresponding demographic and biometric information.[247] According to the Aadhaar Act, the collection, collection, and usage of personal data is a requirement for receiving a subsidy, benefit, or facility.[248] Although this Act does not make

---

makes an application for enrolment: Provided that if an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of the subsidy, benefit or service.

[243] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 8(1) states:- *The Authority shall perform authentication of the Aadhaar number of an Aadhaar number holder submitted by any requesting entity, in relation to his biometric information or demographic information, subject to such conditions and on payment of such fees and in such manner as may be specified by regulations.*

[244] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 8(2) states:- *A requesting entity shall-*
(a) unless otherwise provided in this Act, obtain the consent of an individual before collecting his identity information for the purposes of authentication in such manner as may be specified by regulations; and
(b) ensure that the identity information of an individual is only used for submission to the Central Identities Data Repository for authentication.

[245] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 11(1) states:- *The Central Government shall, by notification, establish an Authority to be known as the Unique Identification Authority of India to be responsible for the processes of enrolment and authentication and perform such other functions assigned to it under this Act.*

[246] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 10 states:- *The Authority may engage one or more entities to establish and maintain the Central Identities Data Repository and to perform any other functions as may be specified by regulations.*

[247] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 2(h) states:- *"Central Identities Data Repository" means a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto.*

[248] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 7 states:- *The Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of, the Consolidated Fund*

application for an Aadhaar Number compulsory *per-se* (i.e.it is specifically provided as a "entitlement" under Section 3 of the Aadhaar Act) except for certain benefits, subsidies, and services funded by the Consolidated Fund of India, in actuality, obtaining and disclosing an Aadhaar Number has become mandatory for availing most services through a variety of cognate regulations.

To ensure the security of information and the privacy of Aadhaar Number holders, the Aadhaar Act and its regulations recognise certain data protection principles, like primarily, the UIDAI is required to ensure the confidentiality and security of individual citizen's identity information and authentication records, which requires taking all necessary steps to safeguard such information against unauthorised access, use, or disclosure, as well as accidental or deliberate destruction, loss, or damage[249]. Furthermore, the Aadhaar Act prevents the sharing and use of core biometric data for purposes other than the creation of Aadhaar numbers[250]. Also under certain conditions, the Act provides that information other than core biometric information may be shared. The Aadhaar Act importantly, allows an individual to access identity information (except core biometric information)[251] and authentication records.[252] The individual can also request that the demographic data be corrected if it changes or is incorrect, as well as the biometric information if it is

---

of India, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment: Provided that if an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of the subsidy, benefit or service.

[249] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 28(3) states:- *The Authority shall take all necessary measures to ensure that the information in the possession or control of the Authority, including information stored in the Central Identities Data Repository, is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage.*

[250] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 29(1) states:- *No core biometric information, collected or created under this Act, shall be—*
(a) shared with anyone for any reason whatsoever; or
(b) used for any purpose other than generation of Aadhaar numbers and authentication under this Act.

[251] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 28(5) states:- *Notwithstanding anything contained in any other law for the time being in force, and save as otherwise provided in this Act, the Authority or any of its officers or other employees or any agency that maintains the Central Identities Data Repository shall not, whether during his service or thereafter, reveal any information stored in the Central Identities Data Repository or authentication record to anyone.*

[252] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 32(2) states:- *Every Aadhaar number holder shall be entitled to obtain his authentication record in such manner as may be specified by regulations.*

misplaced or changes.[253] Interestingly, the Act states that UIDAI will be unaware of the reason for any authentication.[254]

4.3.4.1 The Aadhaar (Data Security) Regulations, 2016 ("Aadhaar Security Regulations") :

The Aadhaar (Data Security) Regulations, 2016 **("Aadhaar Security Regulations")** framed under the *Aadhaar Act*, contain data protection standards for the personal information collected under the Aadhaar Act. These Regulations require the UIDAI to have a security policy outlining the technical and organisational measures it will take to keep information secure.[255]

Despite its efforts to incorporate various data protection principles, the Aadhaar Act has received widespread public criticism. Primarily, despite appearing to be voluntary, Aadhaar possession has become mandatory in actuality, and many see it as the Government's coercive collection of personal data. Concerns have also been expressed about the provision on Aadhaar based authentication, which allows information about an individual to be collected every time a validation request is made to the UIDAI. Finally, despite the requirement to implement adequate security safeguards, no database is completely secure.

---

[253] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 31 states :- *(1) In case any demographic information of an Aadhaar number holder is found incorrect or changes subsequently, the Aadhaar number holder shall request the Authority to alter such demographic information in his record in the Central Identities Data Repository in such manner as may be specified by regulations.*
(2) In case any biometric information of Aadhaar number holder is lost or changes subsequently for any reason, the Aadhaar number holder shall request the Authority to make necessary alteration in his record in the Central Identities Data Repository in such manner as may be specified by regulations.

[254] The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, Section 32(1) states:- The Authority shall maintain authentication records in such manner and for such period as may be specified by regulations.

[255] The Aadhaar (Data Security) Regulations, 2016, Regulation 3(1) states, *Measures for ensuring information security* :- *The Authority may specify an information security policy setting out inter alia the technical and organisational measures to be adopted by the Authority and its personnel, and also security measures to be adopted by agencies, advisors, consultants and other service providers engaged by the Authority, registrar, enrolling agency, requestingentities, and Authentication Service Agencies.*

In addition to the foregoing, certain respective sector specific regulators specify the data privacy provisions that must be implemented by: (i) telecom companies, (ii) banking organisations, (iii) healthcare professionals, and (iv) insurance providers, in order to protect the privacy of data obtained from users and to avoid any non-authorised disclosures to third parties.

The sector specific regulations providing for data protection are specified as follows:

4.3.5 Telecommunications Sector:

The Indian Telegraph Act, 1885 **("Telegraph Act"),** *the Indian Wireless Telegraphy Act, 193 and the Telecom Regulatory Authority of India Act, 1997* **("TRAI Act"),** and various regulations issued pursuant to thereto are all in effect in the telecom sector. However, data protection standards in the telecom sector are primarily governed by the *Unified License Agreement* **("ULA")** issued by the *Department of Telecommunications* **("DoT")**[256] to *Telecom Service Providers* **("TSP")**.

The DoT specifies the format and types of information that must be collected from the individual[257] and the TSP is required to take the necessary precautions to protect the privacy and confidentiality of the data of individuals to whom it offers a service and from whom it has obtained such information.as a result of the service provided.[258] Furthermore, the TSPs are required to keep all business, call detail, exchange detail, and IP detail records for at least two years for DoT review.[259]

---

[256] License Agreement For Unified License, available at : https://dot.gov.in/sites/default/files/UL%20AGREEMENT%20with%20Audiotex%20M2M%20without%20INSAT%20MSSR%2017012022.pdf (Last accessed on October 28, 2022).

[257] License Agreement For Unified License, Clause 39.17(ii) states:-*Format prescribed by the Licensor delineating the details of information required before enrolling a customer as a subscriber shall be followed by the Licensee. A photo identification of subscribers shall be pre-requisite before providing the service. The Licensor may prescribe service-wise detailed instructions for enrolment of subscriber and activation of service from time to time.*

[258] License Agreement For Unified License, Clause 37.2 states:- *Subject to terms and conditions of the license, the Licensee shall take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and its business to whom it provides the Service and from whom it has*

In terms of security safeguards it provides that, the TSP is bound by a number of obligations, including, among other things, inducting only network elements into its telecom network that have been tested in accordance with current Indian or International Security Standards.[260]

Ultimately, customer information can be divulged only if the person has consented to it and the disclosure is in accordance with the terms of the consent. Furthermore, it provides that the TSP must make efforts to comply with the Telegraph Act, which requires the TSP to assist the Government in carrying out message interception in the event of an emergency. This interception process includes some procedural safeguards.[261]

Interestingly, to deal with unsolicited commercial communications, the TRAI has drafted the *Telecom Commercial Communication Preference Regulations, 2010* **("TRAI Regulations")**[262], which mandate the TSPs to establish a *Customer*

---

acquired such information by virtue of the Service provided and shall use its best endeavors to secure that: a) No person acting on behalf of the Licensee or the Licensee divulges or uses any such information except as may be necessary in the course of providing such Service to the Third Party; and b) No such person seeks such information other than is necessary for the purpose of providing Service to the Third Party.

Provided the above para shall not apply where: a) The information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent; or b) The information is already open to the public and otherwise known.

[259] License Agreement For Unified License, Clause 39.20 states:- *The Licensee shall maintain all commercial records/ Call Detail Record (CDR)/ Exchange Detail Record (EDR)/ IP Detail Record (IPDR) with regard to the communications exchanged on the network. Such records shall be archived for at least two year for scrutiny by the Licensor for security reasons and may be destroyed thereafter unless directed otherwise by the Licensor. Licensor may issue directions /instructions from time to time with respect to CDR/IPDR/EDR.*

[260] License Agreement For Unified License, Clause 39.7 states**:-** *The LICENSEE shall induct only those network elements into its telecom network, which have been got tested as per relevant contemporary Indian or International Security Standards e.g. IT and IT related elements against ISO/IEC 15408 standards, for Information Security Management System against ISO 27000 series Standards, Telecom and Telecom related elements against 3GPP security standards, 3GPP2 security standards etc. The certification shall be got done only from authorized and certified agencies/ labs in India or as may be specified by the Licensor. The copies of test results and test certificates shall be kept by the LICENSEE for a period of 10 years from the date of procurement of equipment.*

[261] *Ibid* at 260.

[262] The Telecom Commercial Communications Customer Preference Regulations, 2010, available at; https://www.trai.gov.in/sites/default/files/201205301159277252627regulation1dec2010.pdf,(Last accessed on October 28, 2022).

Preference Registration Facility[263] through which customers can opt out of receiving commercial communications on their mobile devices. These regulations, however, are limited to messages and other forms of communication via phones and would not apply to an email application or advertisements displayed on web browsers.

4.3.6 Financial Sector:

Financial information is a highly sensitive type of information, and requires an adequate data protection regime to ensure its security. Presently in India, *the Credit Information Companies (Regulation) Act, 2005* **("CIC Act")**, *the Credit Information Companies Regulation, 2006* **("CIC Regulations")**, and circulars issued by the *Reserve Bank of India* **("RBI")** are the primary legal regulations addressing data protection in the financial sector. Furthermore, the SPDI Rules also classify financial information such as credit card, debit card, as well as other payment instrument information as "sensitive personal data" governing their use, collection, and disclosure to that extent.

4.3.6.1 The Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983 ("PFI Act"):

In terms of the *Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983* **("PFI Act")**, a public financial institution must not, except as otherwise provided in any other law in force, disclose any information pertaining to, or concerning, the affairs of its components, except in conditions where it is necessary

---

[263] The Telecom Commercial Communications Customer Preference Regulations, 2010 ,Regulation 3(1) states:- *Setting up of Customer Preference Registration Facility:*
Every Access Provider shall set up a Customer Preference Registration Facility, both for wireless and wireline, for registration or deregistration of their preference 5 regarding receipt of commercial communication, in the Provider Customer Preference Register. Provided that any facility set up under sub regulation (1) of regulation 3 of Telecom Unsolicited Commercial Communications, 2007 (4 of 2007) shall continue for the purpose of this sub-regulation and deemed to have been set up under these regulations.

or appropriate for the public financial institution to do so in accordance with the laws or practise and usage customary among bankers.[264]

Further, in terms of the PFI Act, every director, member of any committee, auditor or officer, or any other employee of a public financial institution to which the PFI Act applies must make a declaration of fidelity and secrecy in the form prescribed by the PFI Act before beginning duties.[265]

4.3.6.2 Credit Information Companies (Regulation) Act, 2005 ("CIC Act") and Credit Information Companies Regulations, 2006 ("CIC Regulations") :

The Credit Information Companies (Regulation) Act, 2005 **("CIC Act")** is primarily applicable to *Credit Information Companies* **("CICs")** and recognises them as information collectors[266]. The CIC Act requires CICs to adhere to privacy principles during the collection, use, and disclosure of credit information[267], and to

---

[264] The Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983, Section 3(1) states**:-** *Obligation as to fidelity and secrecy.—(1) A public financial institution shall not, except as otherwise provided in sub-section (2) or in any other law for the time being in force, divulge any information relating to, or to the affairs of, its constituents except in circumstances in which it is, in accordance with the law or practice and usage, customary among bankers, necessary or appropriate for the public financial institution to divulge such information.*

[265] The Public Financial Institutions (Obligation As To Fidelity And Secrecy) Act, 1983, Section 4 states:-. *Declaration of fidelity and secrecy –*
Every director, member of any committee, auditor or officer or any other employee of a public financial institution to which this Act applies, shall,—
(a) before entering upon his duties; or
(b) where he has entered upon his duties as such before the date on which this Act became applicable to such institution, within thirty days from the date on which this Act became applicable to such institution, make a declaration of fidelity and secrecy in the form set out in the Schedule to this Act.

[266] The Credit Information Companies Regulations, 2006, Regulation 2(b) states:- "*collector"" means a credit institution, or a credit information company, or a specified user, as the case may be, which collects data, information, or credit information in respect of a borrower, or a client.*

[267] The Credit Information Companies (Regulation) Act, 2005, Regulation 20 states:- *Privacy Principles :*
Every credit information company, credit institution and specified user, shall adopt the following privacy principles in relation to collection, processing, collating, recording, preservation, secrecy, sharing and usage of credit information, namely:-
(a) the principles—
(i) which may be followed by every credit institution for collection of information from its borrowers and clients and by every credit information company, for collection of information from its member credit institutions or credit information companies, for processing, recording, protecting the data relating to credit information furnished by, or obtained from, their member credit institutions or credit information companies, as the case may be, and sharing of such data with specified users;
(ii) which may be adopted by every specified user for processing, recording, preserving and protecting the data relating to credit information furnished, or received, as the case may be, by it;

ensure that credit information held by them is accurate, complete, and secure against unauthorised use, loss, access, and disclosure.[268]

It is to be noted that the CIC Act[269] also requires a credit information company, credit institute, and specific users to take steps to safeguard the accuracy and security of credit information, including ensuring that the data relating to credit information maintained by them is accurate, complete, and adequately protected against loss, illegal access or use, or unlawfully disclosure.

Similarly, the Act also requires that every CICs, credit institution, and designated user adopt privacy principles in relation to credit card information, including the collection, processing, compiling, recording, retention, secrecy, sharing, and use of credit information.

Similarly, the CIC Regulations require CICs to maintain data security and confidentiality. It also requires them to follow a certain widely accepted data protection principles, such as data gathering, data use, data accuracy, data retention,

---

(iii) which may be adopted by every credit information company for allowing access to records containing credit information of borrowers and clients and alteration of such records in case of need to do so;

(b) the purpose for which the credit information may be used, restriction on such use and disclosure thereof;

(c) the extent of obligation to check accuracy of credit information before furnishing of such information to credit information companies or credit institutions or specified users, as the case may be;

(d) preservation of credit information maintained by every credit information company, credit institution, and specified user as the case may be (including the period for which such information may be maintained, manner of deletion of such information and maintenance of records of credit information);

(e) networking of credit information companies, credit institutions and specified users through electronic mode;

(f) any other principles and procedures relating to credit information which the Reserve Bank may consider necessary and appropriate and may be specified by regulations.

[268] The Credit Information Companies (Regulation) Act, 2005, Regulation 19 states:- *Accuracy and Security of credit information*:- *A credit information company or credit institution or specified user, as the case may be, in possession or control of credit information, shall take such steps (including security safeguards) as may be prescribed, to ensure that the data relating to the 12 credit information maintained by them is accurate, complete, duly protected against any loss or unauthorised access or use or unauthorised disclosure thereof.*

[269] *Ibid* at 268.

and access and alteration. [270]

Further, the CIC Regulation specifies that, in addition to the provisions of CIC Act, every CICs, credit institution, and designated user shall adopt the following privacy principles in their operations: (a) Care in gathering of credit information by ensuring that it is correctly and precisely recorded, compiled, and processed, shielded against loss, illegal access, use, alteration, or disclosure of same (b). Keep the credit information it provides up to date, accurate, and complete (c). Establish and implement procedures for disclosing a person's credit information upon his request and subject to his satisfactory identification (d). Keep credit information collected, maintained, and disseminated by them for at least seven years[271] and, (e). Develop guidelines and procedures for them to follow in terms of credit information preservation and destruction, with the approval of the RBI.

4.3.6.3 Circulars issued by the Reserve Bank of India ("RBI"):

The *Reserve Bank of India* **("RBI")** issues various circulars and regulations, which regulate the functioning of the Banking Sector. The *Know Your Customer* **("KYC")** regulations issued by the RBI restrict the types of information that financial institutions and banks can obtain from their customers.[272]

---

[270] The Credit Information Companies Regulations, 2006, Regulation10 states**:-** *In addition to the principles and procedures as provided in section 20 of the Act, every credit information company, credit institution and specified user, shall adopt the following privacy principles in relation to their functioning, namely:—*
(a) Care in collection of credit information:
(i) Every credit information company shall take all such necessary precautions, in respect of information received or collected by it so as to ensure that such information is:—
(A) properly and accurately recorded, collated and processed; and
(B) protected against loss, unauthorised access, use, modification or disclosure thereof.

[271] The Credit Information Companies Regulations, 2006, Regulation10(d) states:- *Length of preservation of credit information :*
(i) Every credit information company and credit institution shall retain credit information collected, maintained and disseminated by them for a minimum period of seven years.

[272] RBI Master Direction on Know Your Customer (KYC) Direction 2016, dated 25 February 2016, updated as on 8 July 2016, available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10292&Mode=0, (Last accessed on November 23, 2018).

Banks are required to keep such information confidential once it has been collected.[273]

Furthermore, multiple instruments, such as the *Master Circular on Credit Card, Debit Card, and Rupee Denominated Co-branded Prepaid Card Operations of Banks and Credit Card Issuing Non Banking Financial Companies*[274], *the Master Circular on Customer Services, 2009*[275], and the *Code of Banks Commitment to Customers*[276], provide for privacy and customer nondisclosure obligations that must be met by various finance sector entities.

4.3.7 Medicine and Healthcare Sector:

Despite the fact that health information is inherently sensitive, the legal framework in India for data protection in the medicine and health sector seems to be inadequate. Nevertheless, there are certain legislations which are intended to safeguard the personal information of the patient, which are as follows:

4.3.7.1 The Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations, 2002 ("IMC Code"):

The Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations, 2002 **("IMC Code")** promulgated under the *Indian Medical Council Act, 1956*, requires physician-patient confidentiality unless the patient consents or if

---

[273] RBI Master Circular on Customer Service in UCBs dated 1 July 2015, available at: https://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=9863 (Last accessed on November 23, 2018).

[274] RBI Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card Operations of Banks and Credit Card issuing NBFCs, *See also*, Master Circular on Credit Card, Debit Card and Rupee Denominated Cobranded Prepaid Card operations of banks dated 1 July 2014, available at: https://rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=8998 (Last accessed on November 23, 2018).

[275] RBI Master Circular on Customer Service in Banks, 2015 dated 1 July 2015, available at: https://rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=9862 (Last accessed on November 24, 2018).

[276] Code of Bank's Commitment to Customers, Privacy and Confidentiality, Banking Codes and Standards Board of India (June 2014), available at: https://www.dbs.com/in/iwov-resources/pdf/codeofbanks-aug091.pdf (Last accessed on November 24, 2018).

a serious and recognised risk to an individual or community exists, or if the illness is notifiable.[277]

Interestingly, the IMC Code requires that the patient, the family members, and responsible peers of the patient are made aware of the patient's situation in order to end up serving the best interests[278], enabling for disclosure of personal medical information of the patient without the individual's consent. Furthermore, physicians are urged to digitise medical records, keep them for three years[279], and make them available to patients upon request.[280] However, the IMC Code's limited privacy safeguards and lack of an enforcement mechanism render it largely ineffective in addressing the concerns surrounding health information.

4.3.7.2 The Clinical Establishments (Central Government) Rules, 2012 ("Clinical Establishments Rules"):

The Clinical Establishments (Central Government) Rules, 2012 **("Clinical Establishments Rules")** require clinical establishments in India to keep and provide *Electronic Medical Records* and *Electronic Health Records* of patients,

---

[277] Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations, 2002, Regulation 2.2 states:- *Patience, Delicacy and Secrecy :*
Patience and delicacy should characterize the physician. Confidences concerning individual or domestic life entrusted by patients to a physician and defects in the disposition or character of patients observed during medical attendance should never be revealed unless their revelation is required by the laws of the State. Sometimes, however, a physician must determine whether his duty to society requires him to employ knowledge, obtained through confidence as a physician, to protect a healthy person against a communicable disease to which he is about to be exposed. In such instance, the physician should act as he would wish another to act toward one of his own family in like circumstances.

[278] Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations, 2002, Regulation 2.3 states:- *Prognosis :*
The physician should neither exaggerate nor minimize the gravity of a patient's condition. He should ensure himself that the patient, his relatives or his responsible friends have such knowledge of the patient's condition as will serve the best interests of the patient and the family.

[279] Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations, 2002, Regulation 1.3.1 states:- *Maintenance of medical records: Every physician shall maintain the medical records pertaining to his / her indoor patients for a period of 3 years from the date of commencement of the treatment in a standard proforma laid down by the Medical Council of India and attached as Appendix 3.*

[280] Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations, 2002, Regulation 1.3.2 states*:- Maintenance of medical records:*
If any request is made for medical records either by the patients / authorised attendant or legal authorities involved, the same may be duly acknowledged and documents shall be issued within the period of 72 hours.

effectively mandating the electronic storage of health information.[281]

The SPDI Rules also recognise health information as a type of "sensitive data" and regulates the collection, use, and disclosure of such sensitive personal data. However, as earlier stated, the SPDI Rules apply only to the private sector, leaving the entire public health sector out of its purview

4.3.7.3 The Mental Healthcare Act, 2017 ("MH Act") :

The Mental Healthcare Act, 2017 **("MH Act")** was enacted to provide for mental healthcare and services for persons with mental illness and to protect, promote and fulfil the rights of such persons during delivery of mental healthcare and services.

This Act provides that, a person suffering from mental illness has the right to confidentiality in relation to his mental health, mental healthcare, treatment, and physical healthcare and considers these aspects to be important to the individual. Further, it also provides that all healthcare professionals who provide treatment or care to an individual suffering from mental illness are required to keep all information obtained during such care or treatment confidential.[282]

---

[281] The Clinical Establishments (Central Government) Rules, 2012, Rule 9(iv) states:- *Other conditions for registration and continuation of clinical establishments:*
For registration and continuation, every clinical establishment shall fulfill the following conditions, namely :-
(iv) the clinical establishments shall maintain and provide Electronic Medical Records or Electronic Health Records of every patient as may be determined and issued by the Central Government or the State Government as the case may be, from time to time.

[282] The Mental Healthcare Act, 2017, section 23 states:-
(1) A person with mental illness shall have the right to confidentiality in respect of his mental health, mental healthcare, treatment and physical healthcare.
***(2)** All health professionals providing care or treatment to a person with mental illness shall have a duty to keep all such information confidential which has been obtained during care or treatment with the following exceptions, namely:*
(a) release of information to the nominated representative to enable him to fulfil his duties under this Act;
(b) release of information to other mental health professionals and other health professionals to enable them to provide care and treatment to the person with mental illness;
(c) release of information if it is necessary to protect any other person from harm or violence;
(d) only such information that is necessary to protect against the harm identified shall be released;
(e) release only such information as is necessary to prevent threat to life;

This Act also provides that without the consent of the person with mental illness, no photograph or other relevant data concerning an individual with mental illness currently being treated at a mental-health facility should be shared with the media. Importantly, the right to confidentiality of people suffering from mental illnesses extends to all personal data stored in electronic or digital form in either real or virtual space.[283]

The Hon'ble Supreme Court has held in the case of ***Mr X v Hospital Z*** [284] that the patient's right to privacy and the doctor's obligation to ensure the confidentiality are subject to the protection of the others' health. As a result, in this case, the submission that the appellant was HIV+ was held to not contravene the appellant's privacy rights on the basis that the woman with whom he was to be married was saved in moment by such disclosing and from the risk of becoming infected.

4.3.8 Insurance Sector:

Personal data of an individual plays a significant role in the financial sector, as it can be used to identify patterns and predict potential financial instability of the individual. Moreover *Data Analytics* can be used to identify individuals or households that are at a higher risk of financial instability based on factors such as income, credit score, and spending patterns. This information can then be used for targeted financial outreach by the Insurance Companies, much to the dismay of the individuals.

(f) release of information upon an order by concerned Board or the Central Authority or High Court or Supreme Court or any other statutory authority competent to do so; and (g) release of information in the interests of public safety and security.

[283] The Mental Healthcare Act, 2017, section 24 states:-

(1) No photograph or any other information relating to a person with mental illness undergoing treatment at a mental health establishment shall be released to the media without the consent of the person with mental illness.

(2) The right to confidentiality of person with mental illness shall also apply to all information stored in electronic or digital format in real or virtual space.

[284] Mr. X v. Hospital Z (1998) 8 SCC 296.

The insurance industry is poised with a rapidly growing amount of data from various sources, such as policyholder information, claims data, and data from connected devices. However, this raises ethical and data privacy related concerns around the use of this data in the insurance industry, particularly when it comes to privacy and discrimination, and the provisions that regulate these issues at are as follows:

4.3.8.1 Insurance Regulatory and Development Authority of India (Sharing of Database for Distribution of Insurance Products) Regulations, 2010:

The *Insurance Regulatory and Development Authority of India (Sharing of Database for Distribution of Insurance Products) Regulations, 2010* provides that in terms of these regulations, a referral company[285] that has been approved by the *Insurance Regulatory and Development Authority of India* **("IRDAI")** is required to register with the insurance company and is obligated not to disclose customer information without the customer's advance written consent, and is precluded from providing information of any person/firm/company to whom they have not had any confirmed business agreement.

4.3.8.2 Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015:

The *Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015* stipulate that every insurer must maintain records of insurance policies and pertinent information[286], and that such a system must have the required security features. The ways and preservation of the records

---

[285] Insurance Regulatory and Development Authority of India (Sharing of Database for Distribution of Insurance Products) Regulations, 2010**,** Regulation 2(j) states:- *The term "referral company" has been defined to mean a company formed and registered under the Companies Act, 1956 and approved by the IRDAI under sub-regulation (3) of regulation 6 except as otherwise permitted in these regulations*.

[286] Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015, Regulation 3(1) states*:- Maintenance of Policy and Claims records :*
(1) Every insurer shall maintain a record of every policy issued and a record of every claim made as per section 14 (1) (a) and 14 (1) (b) of the Act.

must be in accordance with the insurers and their board's policy and the policy should include: (a). Processing and electronic preservation of records (b).Privacy and security of insured person and claim information (c).Handling malware and insecurity issues (d).Hardware and software security (e).Backups, incident management, and continuity planning, and (f).Data documentation.

It further requires that the policy should also contain a comprehensive plan for reviewing record maintenance and storage implementation, which will be overseen by the committee on risk management.[287] It importantly provides that the records must only be stored and maintained in data centers located in India.[288]

4.3.8.3 Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017:

The *Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017* requires for insurance companies to have in place adequate security and confidentiality precautions when outsourcing its facilities. It provides that the insurer must be satisfied that the outsourcing service provider's security practices, processes, and control mechanisms should be such as to allow it to maintain the privacy and safety of the policyholder's data even after the contract between the insurer and the outsourcing service supplier expires. The Regulation makes it the insurer's obligation to ensure that any information or data shared with any outsourcing service supplier under the outsourcing contracts remains secure, and the insurer should ensure that the policyholder's information is

---

[287] Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015, Regulation 3(6) states:- *With regard to the maintenance of records in electronic form, the policy referred in sub-regulation (5) of regulation 3 shall inter alia include the following:*
i. Processing and electronic maintenance of records,
ii. Privacy and security of policyholder and claim data,
iii. Handling Virus, Vulnerability issues,
iv. Security of Hardware and Software,
v. Backups, Disaster Recovery and Business Continuity and,
vi. Data Archival.

[288] Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015., Regulation 3(9) states:- *The records including those held in electronic mode, pertaining to all the policies issued and all claims made in India shall be held in data centres located and maintained in India only.*

recovered from the outsourcing service provider and that the service provider does not use the policyholder's data again.[289]

It is pertinent to note that apart from the sector specific laws and policies there are certain other legislations in India which contain provisions pertaining to information privacy of individuals, which are as follows:

4.3.9 The Right to Information Act, 2005 ("RTI Act"):

The Right to Information Act, 2005 **("RTI Act")** was enacted to allow private individuals access to information held by Government authorities, in order to encourage accountability and transparency in the functioning of all Government authorities. However, the RTI Act allows for exceptions to information disclosure in certain instances viz, authorities are not required to provide citizens with details relating to personal information of another person, the revelation of which has no connection to any public activity or interest, or that would cause an unnecessary invasion of the person's privacy, except if the Central Public Information Officer, the State Public Information Officer, or the appellate authority, is satisfied that the larger public interest justifies the disclosure of such information.[290]

---

[289] Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017, Regulation 12 states:- *Confidentiality And Security:*
i. The insurer shall satisfy itself that the outsourcing service provider's security policies, procedures and controls will enable the insurer to protect confidentiality and security of policyholders' information even after the contract terminates.
ii. It shall be the responsibility of the insurer to ensure that the data or information parted to any outsourcing service provider under the outsourcing agreements remains confidential.
iii. *An insurer shall take into account any legal or contractual obligations on the part of the outsourcing service provider to disclose the outsourcing arrangement and circumstances under which Insurer's customer data may be disclosed. In the event of termination of the outsourcing agreement, the insurer should ensure that the customer data is retrieved from the service provider and ensure there is no further use of customer data by the service provider.*

[290] Right to Information Act, 2005, Section 8. (1)(j) states:-*Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen:*
(j) information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information.

This legal provision has also be clarified by the Supreme Court and different High Courts vide several of its decisions, For example, the question before the Hon'ble Supreme Court in ***Girish Ramchandra Deshpande v. Central Information Commissioner and Ors,***[291] was whether matters pertaining to an individual's service professional life and specifics of his assets and liabilities, including movable and immovable assets, etc. can be regarded as personal details as outlined under section 8(1)(j) of the RTI, Act. The Supreme Court ruled that, the efficiency of an employee in the company is an issue in between the employer and the employee, and the specifics sought by the petitioner, which include show-cause notifications and orders of condemnation and/or sanctions, fall within the scope of personal information and information disclosed on tax returns for income will be treated the same way. It can only be divulged if the Central Public Information Officer, State Public Information Officer, or Appellate Authority determines that the greater public interest justifies disclosure.

The issue before the Hon'ble Supreme Court in ***Mr. Surupsingh Hrya Naik v. State of Maharashtra through Additional Secretary, General Administration Department and Ors,***[292] consisted of whether the petitioner could claim privilege or confidentiality in regard of medical records retained by a public authority during his confinement. In this case, the petitioner was a member of the State Assembly. The Hon'ble Supreme Court ruled that the privacy and anonymity required to be maintained of a patient's medical records, including those of a convict, cannot be overruled by the Indian Medical Council (Professional Conduct, Etiquette, and Ethics) Regulations 2002 (Regulations) and if there is a conflict between the Regulations and the RTI Act, the RTI Act's provisions will take precedence over the Regulations.

---

[291] Girish Ramchandra Deshpande v. Central Information Commissioner and Ors (2013)1 SCC 212.

[292] Mr. Surupsingh Hrya Naik v. State of Maharashtra through Additional Secretary, General Administration Department and Ors AIR 2007 Bom 121.

4.3.10 The Criminal Procedure (Identification) Act, 2022:

The Criminal Procedure (Identification) Act, 2022 is a fairly recent legislation and has been enacted by the Central Government to authorise the police officers to capture details like measurements of persons convicted, arrested or facing trial in criminal cases, including their iris and retina scans and even biological samples with certain exceptions[293], and store these for upto 75 years.[294] Interestingly, this Act does not yet provide for measures to safeguard the data of the individuals so collected which can pose to be of potential risk to these individuals in case of misuse.

4.4 INSTANCES OF MISUSE AND VIOLATIONS OF PERSONAL DATA IN INDIA:

Inspite of the sector specific laws and regulations regarding data protection and the recognision of Right to Privacy as a Fundamental Right, there have occurred in the country large number of instances where personal data of citizens is fraudulently obtained and is misused mostly resulting in huge monetary loss to the individual's. The following are some of the instances of data misuse and violations which have occurred in various parts of India:

i. On March 25, 2017, the Bank of Maharashtra, Mumbai filed a complaint against 22 residents of Bhayender, Mumbai, accusing them of hacking the bank's central server in Mumbai and allegedly exploiting a flaw in the Central Government's

---

[293] Criminal Procedure (Identification) Act, 2022, Section 4. (1) states:- *The National Crime Records Bureau shall, in the interest of prevention, detection, investigation and prosecution of any offence under any law for the time being in force; (a) collect the record of measurements from State Government or Union territory Administration or any other law enforcement agencies; (b) store, preserve and destroy the record of measurements at national level; (c) process such record with relevant crime and criminal records; and (d) share and disseminate such records with any law enforcement agency, in such manner as may be prescribed.*

[294] Criminal Procedure (Identification) Act, 2022, Section 4 (2) states:- *The record of measurements shall be retained in digital or electronic form for a period of seventy-five years from the date of collection of such measurement:*

United Payment Interface (UPI) mobile application to steal Rs.1.42 crore. The accused carried out the transactions by exploiting a flaw in the software of the UPI app. The accused did not have enough money in their account, but the bug ensured that multiple transactions totaling Rs. 1 lakh went through without being noticed by the bank.[295]

ii. The Unique Identification Authority of India (UIDAI) stated in response to an RTI query in November 2019 that over 200 websites of the Union and State governments had published demographic Aadhar details. The displayed data included the names and addresses of people who had registered with Aadhar and were recipients of various welfare schemes. The display of Aadhar data in this manner is prohibited by the Aadhar Act, 2016.[296]

iii. Personal information of over 2.2 million users was leaked from the McDonald's India app in March 2017. Names, phone numbers, email addresses, home/office addresses, precise home coordinates, and social profile links were among the information leaked. According to cyber security experts, hackers could use the information to gain access to users' financial information, including credit/debit card information and e-wallet details.[297]

iv. In the aftermath of news reports of spyware developed by the Israel based NSO Group which allowed attackers to inject spyware on phones by ringing up targets using Whatsapp's call function, Whatsapp acknowledged that users could be vulnerable to malicious spyware being installed on phones without their knowledge, and urged users to upgrade to the latest version of the app as well as keep the mobile operating system up to date in May 2019. Whatsapp is one of the most popular messaging apps, with 1.5 billion people using it monthly.

---

[295] *Fraudsters exploit flaw in UPI app, bank loses Rs.1.42 cr: Police complaint*, The Indian Express, Mumbai edition, March 27, 2022, at 1.

[296] *Over 200 Govt sites made Aadhaar data public: UIDAI in RTI reply*, The Indian Express, Mumbai edition, November 20, 2017, at 8.

[297] *McD denies personal infor leak of 2.2m users*, The Times of India, Goa edition, March 20,2017, at 5.

The company has emphasised its high level of security and privacy, with its platform being encrypted end to end.[298]

v. Detectives, lawyers, and Bollywood celebrities have been dragged into the Thane, Maharashtra Police Department's Call Detail Records (CDR) investigation. A person's CDR reveals the number of calls made and received, the phone numbers from which the calls were made or received, the date, time, and duration of the calls. The CDR also stores the phone numbers of SMS messages sent and received by a mobile phone. Most importantly, the records show the location from which the calls were placed.[299]

vi. Whatsapp revealed in October 2019 that journalists and human rights activists in India were being monitored by operators using the Israeli spyware Pegasus. While WhatsApp declined to reveal the identities and "exact number" of those targeted for surveillance in India, it did state that it was aware of those targeted and had contacted each one. Whatsapp is said to have contacted and alerted at least two dozen academics, lawyers, dalit activists, and journalists in India.[300]

vii. Thousands of people are duped when online scammers ask them to invest money on a monthly basis in exchange for skyrocketing returns in less than a year. Almost everyone with an e-mail ID would have received emails declaring them the winners of a $1 million jackpot because their email address was chosen in a random drawing. Such crimes have recently evolved into phishing attacks, in which online links such as urgent data entry for renewing credit cards, etc. appear to be from one's service provider. When a user enters their credentials, the conmen not only steal important classified data, but also their bank balance.[301]

viii. A 23-year-old Borivali (Mumbai) resident working as a management trainee at a major bank was allegedly defrauded of Rs.1.56 lakh after unidentified

---

[298] *Security breach: WhatsApp urges users to upgrade app*, The Indian Express, Mumbai edition, May 15, 2019, at 15.

[299] *CDR case: What can be done with your call record data*, The Indian Express, Mumbai edition, March 26, 2018, at 4.

[300] *Whatsapp confirms: Israeli spyware was used to snoop on Indian journalists, activists*, The Indian Express, Mumbai edition, October 31, 2019, at 1.

[301] Sasikumar Adidamu, *Cyber era: From ease to risks, technical wonder to lifestyle imperative*, The Indian Express, Mumbai edition, March 02, 2018, at 21.

individuals obtained her debit card information and blocked SMS alerts to her phone. Her pin number could also be changed by the fraudsters. When she checked her email, she discovered that Rs.1.56 lakh had been withdrawn from her bank account without her knowledge.[302]

ix. In a Facebook data breach, *Social Captain*, a social media booting service that helps users grow their Instagram follower counts, has leaked thousands of Instagram usernames and passwords to potential hackers. Passwords for linked Instagram accounts were stored in plaintext by Social Captain. A website flaw allowed anyone to view any Social Captain user's profile without logging in or accessing their Instagram login credentials.[303]

x. Another important instance is of gross misuse of personal data by Cambridge Analytica, a federal data analytics, marketing, and consulting firm based in London, UK, that is accused of illegally obtaining Facebook data and using it to determine a variety of federal crusades. These crusades include those of American Senator Ted Cruz and, to an extent, Donald Trump and the Leave-EU Brexit campaign, which resulted in the UK's withdrawal from the EU. In 2018, the Facebook–Cambridge Analytica data scandal was a major disgrace, with Cambridge Analytica collecting the private data of millions of people's Facebook profiles including that of Indians without their permission and using it for Political Advertising. It was defined as a watershed moment in understanding of private data, resulting is calls for stricter laws governing tech companies' usage of private data.[304]

Thus, to conclude, it can be inferred from the analysis of the various legislations, that there exists personal data protection provisions in the present laws in India but the same are scattered across the different sectoral legislations providing for uneven

---

[302] *Cyber crime: Bank employee cheated of Rs.1.5 lakh,* The Indian Express, Mumbai edition, March 11, 2018, at 3.

[303] *Thousands of Instagram users' personal details exposed*, available at: https://www.indiatvnews.com/technology/news-instagram-data-breach-users-data-leaked-584582 (Last accessed on February 04,2020).

[304] Case study: Facebook-Cambridge Analytica data breach scandal, available at: https://fotislaw.com/lawtify/case-study-on-facebooks-data-breach/ (Last accessed on November 26, 2023).

levels of protection to the individual, and importantly despite the fact that the State i.e. the Government is able to exercise substantial coercive power, and despite ambiguous claims to personal data that may not be necessary for its functions, the State remains largely unregulated on this account. In the present age, when one can access any information related to anyone from anywhere at any time this poses new threats to private and confidential information. The right to privacy is now recognised as a fundamental right but its protection, growth and development is presently left to the mercy of the judiciary in India . Where Globalisation has given acceptance to the technology in the whole world the provisions of privacy and data protection are not dealt in an exhaustive manner in the present laws, which fall short of being concerned with both protecting the rights of Indian data subjects and reducing the massive power disparity that now exists between major technology companies and ordinary Indian people when it comes to data collecting. Further, the existing laws are inadequate when it comes to processing of personal data between individuals and the government, and focuses on processing of data only between companies and individuals. For example, when government organs judge data collection and usage relevant to state operations, the various loosely stated exclusions in the existing data protection legislations might permit such monitoring.

Thus, suffice it to say that the present sectoral laws are facing the problem of protection of personal data of individuals and a separate legislation is much needed for data protection striking an effective balance between personal liberties and privacy.

It also needs to be noted that a keystone of the EU GDPR is the stipulation of *"adequacy requirements"* which restrict the transfer of personal data to any third country or international organisation that does not *"ensure an adequate level of protection".* In doing so, the European Commission will consider whether the legal framework prevalent in India where personal data will be sought to be transferred, affords adequate protection to data subjects in respect of privacy and protection of

their data and this will directly impact business in India for organisations that deal with such personal data, hence a separate codified law on the subject is warranted.

Thus, in this chapter, the Researcher has analysed and delved into the various legislations and legal provisions presently existing in India that deal with data or informational privacy of individuals and based on the analysis it can be concluded by stating that although there are the legislations and legal provisions, some of which are sectoral, which deal with data or informational privacy of individuals that have been brought about by the legislature and most importantly, the Judiciary, yet there exists lacunae's and deficiency leading to no fortification of personal data privacy and absence of a robust mechanism to address the issues of breach of personal data or personal information in the country.

In the ensuing Chapter, the Researcher has discussed the key components of Personal Data which are the essential constituents of informational privacy required to form part of a data protection legislation and has undertaken the comparative analysis of these essential constituents in the privacy legislations in the countries where the subject law is mature i.e. Europe, United States of America, and the United Kingdom so as to analyse certain significant characteristics of these components as are included in the current and proposed data protection legislation in India.

CHAPTER 5 - COMPARATIVE ANALYSIS OF KEY COMPONENTS OF PERSONAL DATA PROTECTION FRAMEWORK.

5.1 INTRODUCTION :

In the preceding chapter the Researcher delved into the complexities of India's current data protection regime, allowing the Researcher to form a rational opinion about the present situation in the sphere of data protection and informational privacy in India.

In the present chapter the Researcher will advance to compare some of the significant characteristics of the proposed law governing data protection in India.

The Researcher already has in the preceding chapter considered the approach the Indian Judiciary has chosen to take with respect to the various contours of the right to privacy, therefore the deliberations in the present chapter will be limited primarily to the analyses of the legislation of the proposed privacy laws (presently in bill form) and their ramifications for the impending data protection regulation in India.

The comprehensive examination of the important provisions of the proposed legislation will be crucial in determining the Research's outcome.

With the digital boom in India, the issues relating to protection of data and avoidance of identity theft or fraud are genuine concerns and information on the internet is vulnerable to get misused, therefore, there is a dire need to protect citizens from such online intrusion of privacy. Date Protection law is one such legal document to make known the practices on protecting personal information and have procedures in place for Data Processors that gather, use, disclose, and manages the individual’s data.

Thus a clear, up-to-date, and easily accessible Data Protection law is a great checkpoint for demonstrating the principles of transparency, legitimacy of purpose and proportionality providing users with full assurance and knowledge of what they're getting into and in response to these subject matters, several countries have enacted laws with data protection components having broad cross-border and personal reach.

In India, the evolution of framing a data protection law began with the Report of the *Committee of Experts under the Chairmanship of Justice B.N.Srikrishna on A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians,2018* **("Justice Srikrishna Committee Report")**[304] followed by the *Personal Data Protection Bill, 2019* **("PDP 2019")**[305], the *Report of the Joint Committee on The Personal Data Protection Bill 2019, 2021* **("JPC Report, 2021")**[306]and the proposed *Digital Personal Data Protection Bill,2022* **("DPDPB 2022")**[307] being the latest.

Therefore, given that there are currently only piecemeal legislations in India and the proposed legislation on data protection is under deliberation, some cognition of the important concepts of data protection may be required and thus it becomes imperative to understand some of the key components of Data Protection, which are set out hereunder.

---

[304] REPORT OF THE COMMITTEE OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N.SRIKRISHNA ON A FREE AND FAIR DIGITAL ECONOMY, PROTECTING PRIVACY, EMPOWERING INDIANS,2018, available at: https://www.meity.gov.in/writereaddata/files/ Data_Protection_Committee_Report.pdf (Last accessed on September 20, 2021).

[305] The Personal Data Protection Bill, 2019, available at: 2019https://loksabhadocs.nic.in /Refinput / New_ Reference_Notes/English/13062022_142456_ 102120474.pdf (Last accessed on September 20, 2021).

[306] REPORT OF THE JOINT COMMITTEE ON THE PERSONAL DATA PROTECTION BILL 2019, available at: 2021,https://prsindia.org/files/bills_acts/bills_parliament/2019/Joint_ Committee_on_the_Personal_Data_Protection_Bill_2019.pdf (Last accessed on September 20,2021).

[307] The Digital Personal Data Protection Bill 2022, available at: https://www.meity.gov.in/ writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf (Last accessed on January 14,2023).

5.2 PERSONAL DATA:

The critical element that determines the area of informational privacy is the description of *personal information* or *personal data*. The goal of describing personal data or personal information is to offer details on its applicability in regards to data.

It is often debated as to whether a data protection law should apply only to individual persons or also to data of corporate organisations and juristic persons as well. The EU GDPR for example, is applicable only to *"natural persons*" as the definition of *"personal data"* under the EU GDPR, which is based on the UDHR's definition of a natural person[308] is specifically related to individuals rather than legal or juristic persons, since according to the EU's rights-based framework also it is the human beings that are considered subjects of legal relations,[309] further, data pertaining to a corporate entity that would otherwise deserve to be protected from theft or unauthorised disclosure is not covered by the various international data protection legislations.

Essentially the debate on extending data protection laws to organisations focuses on two issues. Firstly, the narrower issue this is based on the argument that the legislation should extend to organisations, particularly smaller enterprises, because information about the organisation may implicitly be information about the organisation's owners and controllers. Secondly, the wider issue that, organisations have legitimate rights in respect of information about them held by others in the same way that individuals have.

---

[308] Universal Declaration of Human Rights, Article 6 states:- *Everyone has the right to recognition everywhere as a person before the law.*

[309] EU GDPR, Article 4(1) states, *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

It is though argued that existing business and commercial laws have sufficient protective measures that can be relied upon to serve the interests of the organisations or artificial persons, such as criminal legislations, intellectual property right laws, information technology laws, credit-rating legislations and the law of tort, including the action for breach of confidentiality. It needs to be appreciated that groups of individuals also do warrant a certain degree of data protection because information about bodies and associations can often be related to individuals, or that, information about a group may carry with it implications about its members, for example, on matters of solvency or reputation. Furthermore, people belonging to a particular group (e.g. immigrants, ethnic minorities, mentally challenged people) sometimes need additional protection against the dissemination of personal information relating to that group. Collective entities can sometimes be as vulnerable as individuals, and thus should have the same right enjoyed by a natural person to correct erroneous information. For Example, a wrong or misleading credit rating can do as much harm to a trading company as to an individual.[310]

Currently, Norway[311], Austria[312], Iceland[313], Luxembourg[314] and Denmark [315]are the five Western European nations which include both physical and non-physical persons in the "data subject" sections of their data protection legislations.

---

[310] I. N. Walden and R. N. Savage, Data Protection and Privacy Laws: Should Organisations Be Protected? The International and Comparative Law Quarterly,Vol. 37, No. 2 (Apr., 1988), pp. 337-347, Cambridge University Press, available at: https://www.jstor.org/stable/760158 (Last accessed on November 27, 2023).

[311] Lov om personregistre m.m av 9 juni 1978 no.48 (English translation: Act of 9 June 1978 Relating to Personal Data Registers, Council of Europe Info.Doc. CJ-PD (86) 26). Para. 1: *The term 'personal information' shall mean information and assessments which are, directly or indirectly, traceable to identifiable individuals, associations or foundations,* available at: https://lovdata.no/dokument/LTI/lov/1993-06-11-78 (last accessed on November 27, 2023).

[312] Bundesgesetz vom 18 Oktober 1978 uiber den Schutz personenbezogener Daten; Bundesgesetzblatt 1978, pp.3619 et seq. (amended July 1986). (English Translation) Section 3.2: *natural and legal persons or associations of persons under commercial law whether specifically identified or likely to be identifiable*.

[313] Act No.39/1985 with regard to the Systematic Recording of Personal Data (English translation: Council of Europe Info.Doc. CJ-PD (86) 15). Art.l: The present Act applies to any systematic recording of data concerning private affairs of individuals as well as financial affairs of individuals, establishments, concerns or other legal persons which should reasonably and normally be kept secret.

[314] Loi du 31 mars 1979 reglementant l'utilisation des donn6es nominatives dans les traitements informatiques, Journal Officiel du Grand-Duchi du Luxembourg A No.29, 11avril 1979 (English translation: Personal Data (Automatic Processing) Act, Council of Europe Info.Doc. CJ-PD (79) 3). Art.2: Person means any natural person, public or private corporate body or group of persons.

[315] Lov om private registre m.v., Lov nr.293 af 8 juni 1978 (English Translation: Act no. 293 of 08/06/1978). Chapter 1 states: *Registration that includes personal data and where electronic data processing is used, and systematic registration that includes information about the private or financial affairs of persons,*

In the United States, privacy protection tends to concentrate on the interests of the individual, guarding against unwarranted intrusions or disclosure by the Federal Government and other public entities. Controls on the disclosure of personal information by Federal agencies was introduced in the Privacy Act of 1974.Interestingly no omnibus Privacy Act exists for the private sector, even at State level, in the Unites States however, specific regulations have been enacted dealing with financial information. So far as the issue of non-physical persons is concerned, the 1974 Privacy Act only gives protection to individuals as citizens of the United States, or an alien lawfully admitted for permanent residence, and not to non-physical persons.

In India also the Right to Privacy established in the *Puttaswamy*[316] judgment stems from the *Right to Life and Personal Liberty* secured by Article 21 of the Indian Constitution[317], thus providing for only *natural persons* to be included in a legislation that stems from a fundamental right, such as the *Right to Privacy*. Thus, while a juristic entity has the legal right to assert and exercise specific fundamental rights, the concepts of *dignity* and *autonomy* may not be fully applicable to it. Also most important data protection principles, such as lawful processing and individual inclusion, are inherently derived from the goal of protecting an individual's autonomy and dignity and not that of a juristic entity. It would therefore be difficult to apply these data protection principles to data pertaining to a legal entity.

However, to make the law wider and encompassing, a distinction could be made between corporate data and certain categories of data held by juristic persons that can justifiably be used to identify a specific person thereby rending it also liable for protection.

---

institutions, associations or companies or otherwise information about personal affairs that can b reasonable be requested, withheld from public, may only take place in accordance with the rules in Chapters 2 and 3.

316 *Supra* note 2 at 1.

317 *Supra* note 203.

The Justice Srikrishna Committee Report recommended personal data to mean data about or relating to a *natural person* who is directly or indirectly identifiable[318], which was followed in the PDP 2019 with the recommendation that personal data be defined based on identifiability and that the *Data Protection Authority* **("DPA")** may issue guidance outlining the standards as they apply to different personal data categories in variety of contexts[319], this was retained in the JPC Report 2021. The proposed DPDPB 2022 also considers personal data to mean any data about an individual who is identifiable by or in relation to such data.[320]

This thus illustrates that data pertaining to a corporate entity that would otherwise deserve to be protected from theft or unauthorised disclosure will not be covered by the proposed data protection legislation in India thereby limiting the applicability of the legislation.

5.3 PSEUDONYMISATION AND ANONYMISATION OF DATA :

The techniques of "*pseudonymisation*" and "*anonymisation*" are related to the concept of identifiability of the data.

Pseudonymisation is a technique for masking identities that does not normally alienate data from the scope of personal data. The EU GDPR suggests pseudonymisation as a technique for lowering risk to individuals' data and

---

[318] Justice Srikrishna Committee Report ,2018, Section 2(29) states:- *"Personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.*

[319] The Personal Data Protection Bill, 2019, Section 3(28) states:- *Personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.*

[320] Digital Personal Data Protection Bill,2022, Section 2(13) states:- "*personal data" means any data about an individual who is identifiable by or in relation to such data*.

achieving data protection obligations.[321]In addition, it specifies organisational and technical safeguards in this regard.

Anonymisation, on the other hand, refers to data in which all identifying components have been removed from a set of personal data. No components are left in the information that could be used to re-identify the person involved with reasonable effort.[322]

It is important to therefore note that when data is successfully anonymised, it is no longer considered personal data. As a result, anonymised data falls outside the scope of data protection laws. Anonymisation is a common practise in many processes, particularly in data aggregation. Even so, the degree of such anonymisation is now a contentious issue, with reports of individuals being identified from ostensibly anonymised sets of data.

The Justice Srikrishna Committee Report recommended restricting the applicability of the data protection legislation only to processing of pseudonymised data[323]. The PDP 2019 also followed this but however made the legislation applicable to anonymised data which may be directed by the Central Government to be provided to it to enable better targeting of delivery of services or formulation of evidence based policies.[324] The JPC Report 2021 differed with this and suggested applicability of the legislation to processing of no-personal data including

---

[321] EU GDPR, Article 4(5) states:- *"pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept* separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

[322] Data Protection Act,2018, Recital 26 states:- *The principles of data protection does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.*

[323] Justice Srikrishna Committee Report,2018, Section 2(3) states:- *Notwithstanding anything contained in sub-sections (1) and (2), the Act shall not apply to processing of anonymised data.*

[324] Personal Data Protection Bill, 2019, Section 2(B) states:- The provisions of this Act, shall not apply to the processing of anonymised data, other than the anonymised data referred to in section 91. *See also* Personal Data Protection Bill, 2019, Section 91 (*2*) states-The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed.

anonymised personal data.[325]Interestingly, the proposed DPDPB 2022 makes no reference to pseudonymisation or anonymisation of data and suggests the applicability of the legislation to automated processing of digital personal data, which is either collected online or personal data which is collected offline but later digitised,[326] thus extending the scope of applicability of the Act to even anonymised data, is encouraging as the ramifications of this could be far reaching, as with advancement of analytical tools individuals are identified from even ostensibly anonymised sets of data. For Example, the Internet of Things **("IoT")** is on the threshold of integration into people's lives. The viability of many projects in the IoT still remains to be confirmed but "smart things" are being made available which monitor and communicate with our homes, cars, work environment and physical activities, these different objects separately collect isolated pieces of information. A sufficient amount of data collected and further analysed can reveal specific aspects of individual's habits, behaviours and preferences. Beyond this, analytics based on anonymised information caught in an IoT environment might enable the detection of an individual's even more detailed and complete life and behaviour patterns, including location analytics or the analysis of movement patterns of crowds and individuals. Thus the intended applicability of the DPDPB 2022 to automated processing of even anonymised digital personal data, is definitely a positive approach.

5.4 SENSITIVE PERSONAL DATA:

All data within the category of personal data are not relatively similar. As explained previously, personal data is information about a person's identity. There are also some personal matters within this area that have a higher privacy expectation and

---

[325] JPC Report, 2021, Recommendation 2.25 states:- *The provisions of this Act shall apply to - (d)the processing of non-personal data including anonymised personal data.*

[326] Digital Personal Data Protection Bill,2022, Section 4(1) states:- *The provisions of this Act shall apply to the processing of digital personal data within the territory of India where:*
(a) such personal data is collected from Data Principals online; and
(b) such personal data collected offline, is digitized.

unlawful use of an individual's such personal information can have serious repercussions. As the Supreme Court of India has also pointed out, apart from the harm of invasion of one's privacy, such data, if divulged, may also be the basis of discrimination action.[327] It is thus necessary to identify this sensitive data and protect it more stringently.

Certain types of information are generally mentioned in the set of sensitive information of an individual across countries which include health data, genetic data, biometric data, religious beliefs, racial or ethnic origin, and sexual preference information. These categories are classified as special categories of personal data under the EU GDPR[328] and are transposed in the UK GDPR as well.

In India, the SPDI Rules, recognises certain core categories for protection as sensitive personal data of an individual i.e. (a) passwords (b) financial information such as credit card or bank or debit card or other payment method details (c) physical, physiological, and psychological health condition (d) sexual preference; (e) health records and history and, (f) biometric data.[329] Race or ethnic origin, philosophical ideologies, affiliation in political organisations, and trade union membership are however excluded, which is found included as special categories of personal data under the EU GDPR.

Financial data is another type of data that requires special consideration. Financial data rightly is classified as sensitive data under the SPDI Rules. This is similar to how financial information, such as credit card information, is treated as sensitive information in the United States.[330] Interestingly Financial data, which is mentioned

---

[327] *Supra* note 2 at 1.

[328] EU GDPR, Article 9(1) states:- *Processing of special categories of personal data**:** Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*

[329] *Supra* note 231.

[330] *Supra* note 142.

in the SPDI Rules, is not mentioned as sensitive data in the EU GDPR or the UK GDPR.

The Justice Srikrishna Committee Report has widened the scope of sensitive personal data as considered under the SPDI Rules to include sex life, sexual orientation, genetic data, transgender status, intersex status and caste or tribe and even political affiliations,[331] The PDP 2019 and the JPC Report 2021 retained this. Interestingly, the proposed DPDPB 2022 makes no reference to sensitive personal data however since it considers personal data to mean any data about an individual who is identifiable by or in relation to such data, it can be interpreted to include sensitive personal data as well,[332] nevertheless an independent definition of what constitutes sensitive personal data and the special measures required to protect it would be beneficial as it would confer a higher degree of protection of this data.

It is therefore important to also understand the important aspect of processing of the sensitive personal data.

According to the EU GDPR, the processing of sensitive personal information is expressly forbidden, except with the clear and specific consent of the individual concerned and in circumstances where processing is allowed by the law.[333] The UK

---

[331] Justice Srikrishna Committee Report , 2018, Section 2(35) states:- *Sensitive Personal Data means personal data revealing, related to, or constituting, as may be applicable—*
(i) passwords;
(ii) financial data;
(iii) health data;
(iv) official identifier;
(v) sex life;
(vi) sexual orientation;
(vii) biometric data;
(viii) genetic data;
(ix) transgender status;
(x) intersex status;
(xi) caste or tribe;
(xii) religiousor political belief or affiliation; or
(xiii) any other category of data specified by the Authority under section 22.

[332] *Supra* note 307.

[333] EU GDPR, Article 9(2) states:- *Processing of special categories of personal data : Paragraph 1 shall not apply if one of the following applies:*

GDPR also replicates the EU GDPR in the matter of processing of sensitive personal information and forbids the processing of such information is expressly prohibited, also unless there is the clear and specific permission of the individual concerned, and where processing is permitted by law.[334]

In the US however, though there is no broad definition of what constitutes sensitive data, several sector-specific laws and regulations put safeguards in place where they are deemed necessary, for example, the FTC states that website operators must obtain the user's express explicit consent before using sensitive customer information, which might include financial details, information about children,

---

1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. processing relates to personal data which are manifestly made public by the data subject;
6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

[334] *Ibid* at 327.

health data, and accurate location data.[335] The Fair Credit Reporting Act restricts the use and disclosure of customer reviews and credit card numbers[336]. The HIPAA governs the collection and disclosure of medical information and establishes guidelines for the safeguard of health data.[337]

As a result, the approach of most countries is to recognise and carve out kinds and types of data that are considered sensitive. This is then safeguarded by according specific safeguards that limit their collection, use, and disclosure in order to minimise harm to the individual.

5.5 DATA PROCESSING :

There is a large amount of personal data being processed by public and private entities alike. Further, an important dimension of the right to privacy is civil rights and surveillance, which involves the State. Data protection laws in jurisdictions such as the EU apply to the Government, as well as private entities as far as their processing activities are concerned.

The Supreme Court of India has noted that legitimate state interests must be protected through exclusions in data protection legislation.[338] Thus, limited exclusions may be considered for well-defined types of departments in the public or government sector like the law enforcement and intelligence agencies, as well as organisations in the private sector.

The term "*processing*" is a very broad term that refers to any activity involving data and thus, to provide the widest possible protection, data protection laws around the

[335] *Supra* note at 150.
[336] *Supra* note at 141.
[337] *Supra* note at 152.
[338] *Supra* note 2 at 1.

world have attempted to establish definitions of *data processing* that encompass all accompanying tasks performed on data.

The EU GDPR considers *processing* as any process or set of operations conducted on personal data or sets of personal data whether by automated means or not and includes acquisition, capturing, organisation, structuring, collection, adaptation or modification, information extraction, discussion, utilisation, disclosure by transmitting, dissemination, or otherwise making it available for alignment or amalgamation, limitation, removal, or elimination[339]. This thus expressly considers a vast majority of data related activities and includes manual and processing of data by automation as well.
The UK GDPR follows the EU GDPR description of processing and considers it both in an inclusive and exhaustive sense.[340]

It is thus important to understand that data processing processes are capable of being carried out using both manual and automatic methods. It is necessary to therefore determine whether a data protection law would be applicable to both kinds of processing in this context.

As the EU GDPR even applies to personal data processed entirely or partially by automatic means, it is also applicable to data that is part of or is expected to be part of a "filing system". A filing system is considered as "any organised set of personal information that can be accessed according to defined conditions, whether

---

[339] EU GDPR, Article 4(2) states,:-*'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

[340] Data Protection Act,2018**,** Article 2 states:- *In this Article:*

(a). 'the automated or structured processing of personal data' means:

(i)the processing of personal data wholly or partly by automated means, and

(ii) the processing otherwise than by automated means of personal data whichforms part of a filing system or is intended to form part of a filing system;

(b)'the manual unstructured processing of personal data' means the processing of personaldata which is not the automated or structured processing of personal data.

centralised, decentralised, or geographically dispersed".[341] The UK GDPR follows the EU GDPR definition of the "filing system" as makes the Act applicable to such filing system.

The Justice Srikrishna Committee Report seems to adopt the EU GDPR definition of *"processing"* of personal data[342], but falls short of specifying it applicability to personal data processed entirely or partially by automatic means. The PDP 2019 and the JPC Report 2021 retained this. Interestingly, the proposed DPDPB 2022 makes it clear that processing in relation to personal data would mean an automated operation or set of operations performed on digital personal data,[343] thus specifying the applicability of the proposed legislation to personal data processed entirely or partially by automatic means.

5.6 DATA CONTROLLER AND DATA PROCESSOR:

Responsibility is a fundamental principle of personal data security. A widely used method for translating data protection norms into action is to identify the party accountable for adherence with these norms. In such frameworks, authority over data refers to the ability to make decisions about the content material and use of the personal data. Thus, a *"Data Controller"* is considered to be the entity that has control over data and is accountable for adhering to data regulations. It is the entity that establishes the objectives, purposes and methods for data processing.[344]

---

[341] EU GDPR, Article 4(6) states:- *"filing system", means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.*

[342] Justice Srikrishna Committee Report , 2018, Section 2(32) states*:- "Processing" in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.*

[343] Digital Personal Data Protection Bill,2022 , Section 2(16) states:- "*processing" in relation to personal data means an automated operation or set of operations performed on digital personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.*

[344] EU GDPR, Article 4(7) states*:- 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of*

Whereas, a "*Data Processor*", on the other hand is an entity that is deeply engaged with processing but acts under the authority of the data controller. It is considered to be the entity that processes the data on the Data Controller's behalf.[345]

The EU GDPR uses the concepts of "*Data Controller*", "*Data Processor*", and "*Third Party*" to identify various entities involved in the processing of personal data. It considers "third party" as the entities other than data controllers or data processors that are authorised to process data under the authority of the data controller or data processor.[346] Furthermore, the EU GDPR makes an effort to be specific about the methods to be used when attempting to enter into processing and sub-processing contractual agreements.

All of these appear to necessitate written legal contracts, which will be fostered by data protection authorities' adoption of basic contractual terms.[347]

---

personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[345] EU GDPR, Article 4(8) states:- *'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

[346] EU GDPR Article 4(10) states:- *'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.*

[347] EU GDPR, Article 28 states:- *Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:*

1. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

2. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

3. takes all measures required pursuant to Article 32;

4. respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

5. taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

6. assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

7. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

This method clearly has the benefit of specificity in responsibility allocation and hence is considered to be the most descriptive model. The UK GDPR has adopted these EU GDPR concepts.

The Justice Srikrishna Committee Report does not consider the term "Data Controller" but rather terms it as *"Data Fiduciary"* and includes it to mean any person, including the Government, a company, any juristic entity or any individual who determines the purpose and means of processing of personal data.[348] The PDP 2019 retained this, however the JPC Report 2021 opined that Non-Governmental Organisations also play a significant role in rural areas in terms of collection of data for various purposes and therefore they should be also treated as "Data Fiduciaries" and should come under the purview of the legislation.[349] Interestingly, the proposed DPDPB 2022 has adopted a simplified approach and considers "Data Fiduciary" to include any person who alone or with other persons determines the purpose and means of processing of personal data.[350]

As regards *"Data processor",* the Justice Srikrishna Committee Report recommends it, to mean any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a *data fiduciary*, it however excluded an employee of the data fiduciary from the purview of the legislation.[351] The PDP 2019 retained this, however the JPC Report 2021opined that

---

8. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.
With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

348 Justice Srikrishna Committee Report, Section 2(13) states:- "*Data fiduciary" means 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.*

349 JPC Report, 2021, Recommendation 2.32 states:- *"data fiduciary" means any person, including a State, a company, a non-government organization, juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.*

350 Digital Personal Data Protection Bill,2022 , Section 2(5) states:- "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;

351 Justice Srikrishna Committee Report, Section 2(15) states:- *"Data processor" means any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary.*

Non-Governmental Organisations also process data on behalf of data fiduciaries for various reasons and therefore they should be also treated as *"Data Processors"* and should come under the purview of the legislation[352] it also made the law applicable to the employee of the *Data Fiduciary*. The proposed DPDPB 2022 has adopted a simplified approach and considers *"Data Processor"* to mean any person who processes personal data on behalf of a *Data Fiduciary*[353], thus making no exceptions.

5.7 DATA PRINCIPAL OR DATA SUBJECT:

The development of a regulatory framework requires fairness in which the individual's rights regarding his or her personal data are recognised and adequately protected and the existing imbalance in leverage between individuals and entities that handle such personal data is remedied.

Thus, for the purpose of data protection, it is the individual who is the "*data principal*" or the *"data subject"* as the individual is referred to under the EU GDPR and the UK GDPR, as he or she is the main figure in the digital personal data sphere. The individual's connection with the entities with whom he or she shares her personal data is founded on a fundamental presumption of trust.

The EU GDPR considers a natural person[354] as the data subject and protects fundamental rights and freedoms of such natural persons and in particular their right to the protection of personal data with regard to the processing of their personal data relating to the free movement of personal data. The UK GDPR also adopts this approach albeit for the citizens of UK.

---

[352] JPC Report, 2021, Recommendation 2.32 states:- *"Data processor" means any person, including a State, a company, a non – government organisation, juristic entity or any individual who processes personal data on behalf of a data fiduciary.*

[353] Digital Personal Data Protection Bill,2022 , Section 2(7) states:- *"Data Processor" means any person who processes personal data on behalf of a Data Fiduciary.*

[354] *Supra* note at 309.

An individual expects his or her personal data to be handled fairly, in a way that meets or exceeds her interests and is reasonably predictable. This is a sign of a fiduciary relationship between the Data Principal and the Data Fiduciary or the Data Processor.

Data Principal's thus consider varying levels of trust and loyalty in the digital economy, based on the type of data that is shared, the objective of such sharing, and the entities with which sharing occurs. This translates into an obligation of care for entities to handle such data responsibly and fairly for the specific purpose normally expected by the Data Principals.

Thus, so as to prevent misuse of the trust reposed by the Data Principal, the Data Fiduciary or the Data Processor, as the case may be, must be obligated by law to utilise the personal data assigned to it by the Data Principal solely for the purpose for which the Data Principal reasonably expects it to be utilised.
This commitment to process fairly entails that the Data Fiduciary or the Data Processor must act in the best interests of protection of the Data Principal's privacy.

The Justice Srikrishna Committee Report considers only a natural person to be the Data Principal,[355] and recognises the duty the person processing personal data owes to the data principal to process the personal data in a fair and reasonable manner that respects the privacy of the data principal.[356] The PDP 2019 also considered natural person to be the Data Principal, however it avoids recognising the duty the person processing personal data owes to the data principal. The JPC Report 2021did not make any significant change to this approach. The proposed DPDPB 2022 interestingly does not restrict the applicability of Data Principal to only natural persons but rather considers individuals to whom the personal data relates and in

[355] Justice Srikrishna Committee Report, Section 2(14) states:- *"Data principal" means the natural person to whom the personal data referred to in sub-clause (28) relates.*

[356] Justice Srikrishna Committee Report, Section 4 states:- *Fair and reasonable processing - Any person processing personal data owes a duty to the data principal to process such personal data in a fair and reasonable manner that respects the privacy of the data principal.*

case of a child it considers the parents or lawful guardian of such a child to be the Data Principal[357], though it also avoids mention of the duty the person processing personal data owes to the Data Principal.

5.8 CROSS-BORDER TRANSFER OF DATA:

With the advancement of the Internet, massive amounts of personal data pertaining to individuals, employees and customers are being transmitted across countries globally. Also as many international corporations have customer databases and warehousing facilities in different international locations, such data transfers frequently occur between and among units within the same corporate enterprise that are situated in different countries.

Data transfer across borders is critical for gaining access to crucial digital services. Businesses must be able to send not only products, wealth, and expertise of people across boundaries in order to conduct business, but also digital data to be creative, and remain competitive in international markets. If beneficial laws enabling cross-border data transfer exist, it will significantly boost research, technological development, and economic expansion.

The EU has established three systems to enable cross-border transfer of data. These consist of the EU GDPR's *adequacy test*,[358] *model contractual clauses*,[359] and *binding corporate rules.*[360] Furthermore, the *Privacy Shield Framework*[361] is used for cross-border transfer of data between EU and the US.

---

[357] Digital Personal Data Protection Bill,2022 , Section 2(6) states:- *"Data Principal" means the individual to whom the personal data relates and where such individual is a child includes the parents or lawful guardian of such a child.*

[358] *Supra* note at 131.

[359] *Ibid* at 132.

[360] *Id.*

[361] *Supra* note at 104.

The *adequacy test* under the EU requires that personal data of EU citizens cannot be transferred to *Non-European Economic Area* nations unless such countries have sufficient level of data protection. Furthermore, the EU GDPR also provides that the adequacy standard of a particular third country must be reviewed every four-year basis, if further provides that if the *European Commission* does not take a decision regarding the adequacy level of that other country, it empowers the Data Controller to transfer personal data if adequate safeguarding measures and effective legal remedies for data subjects are provided.[362]

In India, the Justice Srikrishna Committee Report provided for the Cross-Border Transfer of personal data and laid down the conditions of such data transfer but also recommended that the data fiduciary should mandatorily store at least one copy of such personal data on a server or data centre located in India.[363] The PDP 2019 though allowed Cross-Border Transfer of personal data, it in turn suggested enabling restrictions on the transfer of sensitive personal data outside India.[364] The JPC Report 2021did not make any significant change to this approach but offered explanations to effect that Cross-Border Transfer of personal data should not approved by the Central Government if object of such transfer is against public policy or Government policy.[365] The proposed DPDPB 2022 interestingly does not expressly provide for free flow of cross-border transfer of personal data, but rather it grants the authority to the Central Government to notify the countries or territories outside India to which a Data Fiduciary may transfer personal data, naturally based on the subjective satisfaction of the Central Government.[366]

---

[362] *Supra* note at 133.

[363] Justice Srikrishna Committee Report, Section 40(1) states:- *Every data fiduciary shall 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 applies.*

[364] Personal Data Protection Bill, 2019, Section 33 (1) states:- *Subject to the conditions in sub-section (1) of section 34, the sensitive personal data may be transferred outside India, but such sensitive personal data shall continue to be stored in India.* See also Personal Data Protection Bill, 2019, Section 34.

[365] Recommendation No.52 of the JPC Report, 2021.

[366] Digital Personal Data Protection Bill,2022 , Section 17 states:- *The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified.*

5.9 DATA LOCALISATION :

The concept of *data localisation* necessitates that Data Fiduciaries store and process data on servers that are physically situated within the countries national boundaries. Concerns about privacy, safety, electronic surveillance, and law enforcement have prompted Governments around the world to enact legislation requiring data localisation. A nation most certainly is entitled to take measures to safeguard its interests and sovereign rights, but it must carefully consider the benefits and risks of storing data locally before making a deliberate choice on an issue that has the possibilities to have a large cascading effect across a wide range of businesses.

The main reason for enacting a *data localisation* law is to avoid foreign electronic surveillance. It is based on the conviction that data transmitted internationally will indeed allow foreign government entities to infringe on people's privacy and security, as a result, some nations have attempted to prevent data from leaving their borders in order to safeguard it from getting into the hands of other foreign government entities.

In the EU the EU GDPR Act does not mandate the storing of the data locally, however the issue of *data localisation* are adequately addressed based on the *adequacy decisions* of the European Commission.[367] Similar position is adopted under the UK GDPR.

In the financial and telecom sector, India presently has a mandate for data localisation in regards to customer account information. According to the RBI's Directive, entities governed by the RBI must store payment information within

[367] EU GDPR, Recital 103 states:- *Appropriate level of Data Protection based on an Adequacy Decision – The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. [2]In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.*

India[368]. This thus can create some issues with multinational companies seeking to provide consolidation of services and encryption.

And as discussed above, the Justice Srikrishna Committee Report recommended for *data localisation* by providing that the data fiduciary should mandatorily store at least one copy of personal data on a server or data centre located in India.[369] However no such express provision is made either in the PDP 2019, the JPC Report or the proposed DPDPB 2022 which leaves it to the satisfaction of the Central Government to make necessary rules regarding the same.

5.10 CONSENT :

In many countries, "*consent* " is the cornerstone of data protection law. "*Consent*" as a validation and verification mechanism for data processing has substantial value. It is inherently regarded to be the most efficient method for ensuring an individual's personal autonomy. Enabling person autonomy over his or her personally identifiable information makes it possible for him or her to enjoy the informational privacy.

In the *Puttaswamy*[370]case the Supreme Court of India has held that the *right to privacy* includes the *right to informational privacy*, which thus acknowledges that an individual should also have authority over the use and dissemination of its personal information and any unlawful use of this would be a violation of this right.

---

[368] The Reserve Bank of India's Directive 2017-18/153 (April 6, 2018), Para 2(i) states:-
It is observed that not all system providers store the payments data in India. In order to ensure better monitoring, it is important to have unfettered supervisory access to data stored with these system providers as also with their service providers / intermediaries/ third party vendors and other entities in the payment ecosystem. It has, therefore, been decided that:
i. All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required.

[369] *Ibid* at 357.

[370] *Supra* note 2 at 1.

The instruments of *"notice"* and *"choice"* serve to formalise *consent*, they empower the individual to control the collection and usage of its personal information. Thus, instead of stringent regulations over how an individual's data could be used, *consent* is considered to be a more versatile, cost effective and easily enforceable method for safeguarding personal data of individuals as seeking consent empowers the individual to remain in charge of its own data.

Individuals do tend to read the online privacy notice in some cases, but lack the understanding to ascertain the ramifications of consenting to a specific use of their information. This is particularly true in areas of rapidly evolving technology, where it may be challenging for a person to continuously educate oneself about technological advances and, as a result, their implications on their privacy. Eventually, even if people do read and comprehend the details in the notice, they will only be able to make a well-informed decision about the immediate use of their information and they might find it difficult to make an informed choice about the possible future usage of their information and the harmful consequences that may result. All of these aspects lead to a decrease in the value of consent.

Nevertheless the advantage of using "consent" to safeguard personal information is that it takes different privacy principles into account. Individuals are more often in the best position to determine what proportion of their personal information they are willing to share in exchange for the products and services offered by a company.

In terms of the EU GDPR, *"consent"* is the basic foundation for the collection, use, and dissemination of personal information, it stipulates that personal information could be processed on six different grounds, of which *consent* forms the key.[371] To

[371] EU GDPR, Article 6(1) states:- *Processing shall be lawful only if and to the extent that at least one of the following applies:*
a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

ensure that an individual's consent is legitimate, the EU GDPR requires that *consent* be given freely, should be precise, must be informed, and should be unequivocal for the processing of personal information. It also requires that the *consent* must be conveyed through a statement or evident affirmative action.[372]

Importantly, in relation to processing of *sensitive personal data*, the EU GDPR mandates the requirement for a higher degree of *consent* i.e. it requires that consent in such instances be explicit.[373]

Pertinently, the EU GDPR also asserts that the individual is entitled to withdraw *consent* at any point. It importantly provides that the withdrawal of *consent* has no bearing on the legality of the processing carried out based on consent obtained prior to its revocation. It also provides that it should be as simple to withdraw just as it is to give consent.[374] The individual must also provide consent for the processing of his or her private information under the UK GDPR as it complies with the EU GDPR approach by making consent as one of the legal grounds for processing.[375]

In the US, privacy is safeguarded by a patchwork of State and Federal laws where many are industry-specific. *Consent* and *notice* are used extensively in data protection legislations in the US, for example, the GLB Act, which regulates the

---

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

[372] EU GDPR, Article 4(11) states:- *'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

[373] *Supra* note 127.

[374] *Ibid* at 127.

[375] Data Protection Act,2018**,** Recital 42 states, *Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC(10) a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.*

financial services sector, imposes certain responsibilities on financial institutions to obtain consumer consent before gathering non-public financial data and prohibits the release of information of any non-public financial data to a third party in the absence of consumer consent.[376]

In India, presently the *SPDI Rules* require private organisations to obtain the individual's *consent* before capturing or divulging sensitive personal Information to a third party. It further requires that consent to capture sensitive personal information be procured in writing from the provider of such data via letter, fax, or electronic mail, foreseeably making legitimate consent gathering difficult in actuality.[377] It also allows private organisations to transmit *sensitive personal information* outside of India, if the individual consents to the transfer or the private organisation have a contract with that jurisdiction which allows for the transfer of Sensitive personal Information across borders.[378]

Justice Srikrishna Committee Report also attached substantial importance to *consent*, and recommended that the *consent* to be valid has to be free, informed, specific, clear, and revocable.[379] It importantly also provided that the Data Fiduciary should not make the provision of any goods or services, or the enjoyment of any

---

[376] *Supra* note 196.

[377] *Supra* note 237.

[378] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Rule 7 states:- *Transfer of information:*
A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

[379] Justice Srikrishna Committee Report, Section 12(2) states:- *For the consent of the data principal to be valid, it must be -*
(a) free, having regard to whether it meets the standard under section 14 of the Indian Contract Act, 1872 (9 of 1872);
(b) informed, having regard to whether the data principal has been provided with the information required under section 8;
(c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purposes of processing;
(d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and
(e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

legal right, a condition precedent for processing of any personal data.[380] The PDP 2019 followed this, but added that *consent* will have to be clear and unambiguous for processing of sensitive personal data.[381] The JPC Report followed the PDP 2019 with minor alteration.[382] The proposed DPDPB 2022 also provided for the consent to be free, specific, informed and unambiguous, which is conveyed by a clear and affirmative action, and also provided for the Data Principal to give, manage, review or withdraw consent given to the Data Fiduciary through a "Consent Manager", which the legislation defines, is a Data Fiduciary who acts on behalf of the Data Principal, enables the Data Principal to give, manage, review and withdraw its consent through an accessible, transparent and interoperable platform.[383]Interestingly, this legislations provides for *"deemed consent"* [384] which unfortunately may be prone to misuse by private as well as Government.

5.10.1 Consent of a Child:

As can be understood from the analysis above, consent of the Data Principle plays an important part in processing its personal data, this then poses the important question on the consent of a child, who is also a Data Principle.

---

[380] Justice Srikrishna Committee Report, Section 12(3) states:- *The data fiduciary shall not make the provision of any goods or services or the quality thereof, the performance of any contract, or the enjoyment of any legal right or claim, conditional on consent to processing of any personal data not necessary for that purpose.*

[381] Personal Data Protection Bill, 2019, Section 11(3) states:- *In addition to the provisions contained in sub-section (2), the consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained—*
(a) after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal;
(b) in clear terms without recourse to inference from conduct in a context; and
(c) after giving him the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing

[382] Recommendation No.33 of the JPC Report, 2021.

[383] Digital Personal Data Protection Bill,2022 , Section 7(6) states:- *The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager.*
For the purpose of this section, a "Consent Manager" is a Data Fiduciary which enables a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.
See also Digital Personal Data Protection Bill,2022, Section 7(7) states:-*The Consent Manager specified in this section shall be an entity that is accountable to the Data Principal and acts on behalf of the Data Principal. Every Consent Manager shall be registered with the Board in such manner and subject to such technical, operational, financial and other conditions as may be prescribed*.

[384] Section 8 of the Digital Personal Data Protection Bill,2022 .

Today schools and educational establishments are increasingly digitising their operations, frequently implementing cloud-based facilities and software as a service component to manage them. These establishments require clear guidance on how to manage the relevant data they store concerning children, including regulatory requirements on providers of cloud services regarding storage, computation, and transmitting. The Government too collects data concerning children in the course of its different functions, but there are no differential data processing practices in place.

Despite the fact that children are increasingly using the Internet and becoming more acquainted with technology, they are perceived to be more susceptible than adults online. Because they are less conscious of the lasting implications of their online actions, they could be more easily manipulated. As a result, children are a vulnerable population that may benefit from additional safeguards for their personally identifiable information.

Thus, several countries have acknowledged the need to implement measures for data protection that are particularly applicable to the processing of personal information regarding children. The goal of establishing a separate protection framework for services that process children's personal data is fairly obvious, however, determining the precise kind of entity to which it should apply is difficult.

In the US, additional data protection safeguards for children are applicable only to internet sites catering to children, this coverage could be too narrow as the children frequently access social media websites like “Facebook”, which is essentially not a children's website.

COPPA was one of the first acts of legislation enacted in the US to explicitly safeguard the online privacy of minors. COPPA grants parents control over the information online commercial websites obtain from children under the age of 13

years.[385] The FTC has also issued guidance regarding measures to ascertain parental consent.[386]

The EU GDPR expressly states that children require more safeguards than adults because they are much less aware of risks, implications, protections, and their rights regarding processing of their personal data, particularly online. In instances where children's personal data is being processed with their consent, the EU GDPR requires parental consent on internet sites that provide services actively to children below the age of 16 years but recommends that Member States may provide for a lower age of 13 years.[387]

Under the UK GDPR the age of valid consent is lowered to 13 years in the UK[388] which is a notable change from the EU GDPR, it further reiterates that all processing must be legal and fair.[389] As a result, the UK GDPR recommends that data be collected in a manner that the child is most likely to understand, and that the nature and amount of data collected from a child be commensurate to his or her level of comprehension.

In India, the Justice Srikrishna Committee Report considers a data principal below the age of 18 years as a child and recommends processing of personal data of children in a manner that protects and advances the rights and best interests of the

---

[385] Children's Online Privacy Protection Act, 1998, Regulation 6502 states:- *Regulation of unfair and deceptive acts and practices in connection with collection and use of personal information from and about children on the Internet -*
(a) Acts prohibited:
(1) In general-
It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b).

[386] *Supra* note 150.

[387] EU GDPR, Article 8(1) states:- *Conditions applicable to child's consent in relation to information society services :*
Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. [2]Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

[388] *Supra* note 197.

[389] *See Supra* note 118.

child.[390] The PDP 2019 retains these provisions but provides that guardian data fiduciaries that solely provide counseling or such other similar services to children will not be obligated to obtain parental consent.[391]The JPC Report also retained these provisions with minor amendments and suggested defining of the term "guardian data fiduciary" which was left undefined in the PDP 2019.[392]

The proposed DPDPB 2022 has also considered an individual below the age of 18 years as a child but does not lay down any specific safeguard for processing of personal data of children while only providing for obtaining verifiable parental consent.[393]

5.11 USE LIMITATION AND PURPOSE SPECIFICATION:

The important facets of data protections are that the personal data must not be disclosed, it must be not accessible or otherwise used for reasons other than those for which the same is collected and processed. However there could be two specific exemptions to which this may not apply i.e. (a). when the individual has consented to the use or disclosing, and (b.) when such use or disclosing takes place with the legal authority. The purpose of including these two exceptions is to allow for some leeway in data processing activities.

Thus the underlying premise of the *use limitation principle* is data minimisation, or the practise of collecting only the personal information that is required to achieve a specific purpose or objective.[394]

---

[390] Justice Srikrishna Committee Report, Section 12(9) states:- *"Child" means a data principal below the age of eighteen years.*

[391] The Personal Data Protection Bill, 2018, Section 16 (7) states:- *A guardian data fiduciary providing exclusive counselling or child protection services to a child shall not require to obtain the consent of parent or guardian of the child under sub-section (2).*

[392] Recommendation No.38 of the JPC Report, 2021.

[393] Digital Personal Data Protection Bill,2022 , Section 10(1) states:- *The Data Fiduciary shall, before processing any personal data of a child, obtain verifiable parental consent in such manner as may be prescribed.*

[394] Available at: https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection#:~:text=Purpose%20Limitation%3A%20Personal%20data%20should,is%20incompatible%20with%20those%20purposes,(Last accessed on November 02, 2022).

Purpose Specification is a crucial initial step in implementing data protection laws and developing safeguards for the collection, utilisation, and dissemination of personal information. It is intended to define the limits within which personal data obtained for a specific purpose could be processed and used further. This principle consists of two parts i.e. (a). that data must be collected for a specific purpose, and (b). once collected, data should not be processed in a way that is incompatible with the objective for collection and each successive use should be specified at the time of purpose change.[395]

The *purpose specification principle* ensures that organisations are transparent about their purposes for collecting personal data and that their use of the data is consistent with the reasonable expectations of the individuals involved.

The EU GDPR does not provide for the *use limitation principle* independently, it is incorporated into the *purpose specification principle*.

The *purpose specification* principle contemplated by the EU GDPR necessitates that the Data Controller only collects data for specified, explicit, and lawful purposes, and that once obtained, it must not be processed in a way which is inconsistent with the original intent.[396] It further allows further use of the data as long as it is for scientific, historical, or statistical academic purposes which are not regarded incompatible.[397]

The intention is thus to ensure that the organisations collecting the personal data carefully considers the purposes for which the information will be utilised for and to

---

[395] *Ibid* at 388.

[396] EU GDPR, Article 5(1)(b) states, *Personal data shall be :*
collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

[397] EU GDPR, Article 89(2) states, *Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes :*
Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

prevent the collection of information that may not be necessary, adequate, or pertinent for the purpose.

The UK GDPR mirrors the EU GDPR based on which it provides that the data can be obtained only for one or more specific and legitimate purposes, and it may not be further processed in any way that is inconsistent with that purpose and according to the *ICO* guidelines[398], the compatibility of successive use is determined by whether the intended use is legitimate under the UK GDPR.

In India, the Justice Srikrishna Committee Report provided for the *purpose limitation* and *collection limitation* by recommending that personal data should be processed only for specified purposes that the data principal would reasonably expect the personal data to be used for, and the context and circumstances in which the personal data was collected and further limiting the collection of such data only as is necessary for the purposes of processing.[399] The PDP 2019 retained this recommendation, which the JPC Report made minor amendments to the same.[400]The proposed DPDPB 2022 however surprisingly makes no mention *of* either the *use limitation* or *purpose specification* thus leaving it open for interpretation.

5.12 DATA PORTABILITY

Data portability is the ability to move data among different application, programs, computing environments or cloud services. In a cloud computing context, data portability is one part of cloud portability, which makes it possible for customers to

---

[398] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/?template=pdf&patch=248#link7 (Last accessed on November 11, 2022).

[399] Justice Srikrishna Committee Report, Section 5(2) states:- *Personal data shall be processed only for purposes specified or for any other incidental purpose that the data principal would reasonably expect the personal data to be used for, having regard to the specified purposes, and the context and circumstances in which the personal data was collected.* See also Justice Srikrishna Committee Report, Section 6 states:- *Collection of personal data shall be limited to such data that is necessary for the purposes of processing.*

[400] Recommendation No.29 of the JPC Report, 2021.

migrate data and applications between or among *Cloud Service Providers* **("CSPs")**.

Data portability is becoming more important as an increasing number of organisations store greater quantities of data in the cloud. Of course, the requirement to move and transfer data in a portable format is not limited to cloud computing, it applies to other premises and other forms of information technology as well.

For consumers, data portability lets people easily coordinate the personal data they keep on multiple social networking sites. On social networking sites, such as Facebook, LinkedIn and Twitter, users can share their contacts, posts, photos, videos, sound clips and personal or professional information across the various platforms. In that way, users know their data is current and consistent, without having to modify the content on each service's site.[401]

There is no standard, universal right to data portability, the EU GDPR however recognises the importance of data portability and provides to the data subject the right to have the personal data transferred from one data controller to another, where data portability is technically possible, It also importantly provides this right to the data subject, without hindrance from the controller to which the personal data was initially provided.[402]This position has been adopted in the UK GDPR as well.

---

[401] Craig S. Mullins, Mullins Consulting, data portability, available at: https://www.techtarget.com/searchcloudcomputing/definition/data-portability (Last accessed on May 20, 2023).

[402] EU GDPR, Article 20 states:- 1. *The data subject shall have the right to receive the 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 have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:*

a. the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

b. the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

In the US, it is the *California Consumer Privacy Act* (CCPA) that accords the right of data portability to the consumer under the right to access and provides that electronic data must be provided by the businesses to the consumer in a portable format that, if technically feasible, that will further enable the consumer to transmit it further.[403]

The Justice Srikrishna Committee Report recognised data portability and included it as a right of the data subject.[404] The PDP, 2019 and the JPC Report retained this recommendation. Ironically however, the proposed DPDPB 2022 does not grant the right to data portability to the data principal, thus deterring the protection to data interoperability and migrating data by the individuals. For instance, India presently provides for Mobile Number portability from one Telecom Provider to another and also Insurance Policy portability from one Insurance Provider to another, however when opting for such "porting", individuals have to submit their personal identifiable data like Aadhar Card afresh to the new Service Provider, and there is presently no legal mechanism to find out what has happened to their personal data held by the earlier Service Provider. Grant of the Right to Data Portability in the proposed DPDPB 2022 could have given the individuals the right to receive personal data they provided to the earlier Service Provider in a structured, commonly used and machine readable format. It could also have give the individuals the right to request that that the earlier Service Provider transmit this data directly to another Service Provider, while making the earlier Service Provider responsible for the transmission by taking appropriate measures to ensure that it is transmitted securely and to the right destination.

Arguably if the proposed DPDPB 2022 had granted the right to data portability to the data principal, it would have allowed individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.

---

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

[403] *Supra* note 167.

[404] Section 26 of the Justice Srikrishna Committee Report.

5.13 DATA PROTECTION AUTHORITY :

Though data protection legislation may well be enacted to protect individuals, its application and effectiveness is dependent on the establishment of an effective, independent, and technically proficient competent authority tasked with the duty to protect and adjudicate on the matter of data protection. This is especially true when it comes to data protection challenges, which can be highly specialised and necessitate expertise in a variety of fields such as data analytics, data science, legislation, and related issues.

Several nations have transitioned from a comprehensive and multi regulatory structure to a more streamlined national agency structure as regards the *Data Protection Authority*. The advantages of a single, centralised regulatory authority appears to be significant, particularly in the context of international business opportunities, because multinational companies can have a single point of contact and such an authority can ensure the consistency by issuing an uniform set of rules, guidelines, or standards. Furthermore, a single, centralised regulatory authority makes it easier for individuals to seek guidance and direct questions and complaints in regards to a data protection violation.

The EU GDPR contemplates the establishment of one or more supervisory authorities within every EU Member State to enforce compliance with the EU GDPR's regulations.[405] Accordingly, Member States have the option to choose the credentials, eligibility conditions, and procedures and rules for appointing members of the Data protection Authority i.e. termed as the *Supervisory Authority*.[406]

---

[405] EU GDPR, Article 51(1) states:- *Supervisory Authority* –
Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

[406] EU GDPR, Article 53 states:- *General conditions for the members of the supervisory authority* -
1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:
– their parliament;
– their government;

The EU GDPR also guarantees the service period of each member of this Supervisory Authority by providing a fixed tenure of not less than four years.[407] The EU GDPR includes specific provisions for guaranteeing the independence of supervisory authority members.[408]Furthermore, a member may be dismissed only for serious misconduct if the member no longer meets the conditions for performing his or her duties.[409] The *Supervisory Authority's* functions, obligations, and powers under the EU GDPR include the following :

(a). inspection, enforcement, and investigation,[410] (b). corrective authority[411], and (c). advisory powers.[412]

– their head of State; or

– an independent body entrusted with the appointment under Member State law.

2. *Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.*

[407]EU GDPR, Article 54(d) states, *Rules on the establishment of the supervisory authority –*
the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure.

[408] EU GDPR, Article 52 states, *Independence -*
Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

1. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

2. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

3. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

4. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

5. *Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.*

[409]EU GDPR, Article 53(4) states:- *General conditions for the members of the supervisory authority –*
A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

[410] EU GDPR, Article 58(1) states:- *Powers –*
Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f)to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

The UK-GDPR follows all the specific provisions for guaranteeing the independence of the *Supervisory Authority* as stipulated under the EU-GDPR, and achieves it by the appointment of an *Information Commissioner*[413] who is responsible for enforcing the obligations imposed under the UK GDPR.

---

[411] EU GDPR, Article 58(2) states, *Powers* –
Each supervisory authority shall have all of the following corrective powers:
(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
(e) to order the controller to communicate a personal data breach to the data subject;
(f) to impose a temporary or definitive limitation including a ban on processing;
(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
(j) *to order the suspension of data flows to a recipient in a third country or to an international organisation.*

[412] EU GDPR, Article 58(3) states, *Powers* –
Each supervisory authority shall have all of the following authorisation and advisory powers:
(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;
(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;
(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);
(e) to accredit certification bodies pursuant to Article 43
(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);
(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);
(h) to authorise contractual clauses referred to in point (a) of Article 46(3);
(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);
(j) *to approve binding corporate rules pursuant to Article 47.*

[413] Data Protection Act, 2018 Section 114 (1), states:- *The Information Commissioner* –
There is to continue to be an Information Commissioner
See also, Data Protection Act, 2018 Article 52 states, *Independence* -
The Commissioner shall act with complete independence in performing tasks and exercising powers in accordance with this Regulation.
The Commissioner shall, in the performance of tasks and exercise of powers in accordance with this Regulation, remain free from external influence, whether director indirect, and shall neither seek nor take instructions from anybody.
The Commissioner shall refrain from any action incompatible with the Commissioner's duties and shall not, while holding office, engage in any incompatible occupation, whether gainful or not.

Thus, eventually any legislation is only as good as its implementation. A competent enforcement mechanism is critical to ensuring that India too has a strong data protection system that ensures that its substantive obligations are adhered to.

Presently, there is no independent authority in India to safeguard compliance with data protection responsibilities. The extent of the IT Act is restricted, and it provides for the appointment of adjudicating officers[414] and an appellate mechanism[415], the primary mandate of which is to adjudicate disputes that arise under the IT Act. As a result, a stronger framework in the form of a central, oversight authority may be necessary in India in order to achieve effective personal data protection.

The Justice Srikrishna Committee Report provided for the establishment of a Data Protection Authority Of India, but recommended that the chairperson and the members of the Authority to be appointed by the Central Government on the recommendation made by a selection committee and the procedure to be followed by the selection committee for recommending these names shall be such as may be prescribed by the Central Government, thus in effect diluting the independence of the Authority.[416] The PDP 2019 retained this recommendation, which the JPC Report made minor amendments to the same. The proposed DPDPB 2022 however has provided for a Data Protection Board of India, which stating that the strength and composition of the Board and the process of selection, terms and conditions of appointment and service, removal of its Chairperson and other Members shall be

---

[414] The Information Technology Act, 2000, Section 46(1) states:- *Power to Adjudicate: For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder which renders him liable to pay penalty or compensation, the Central Government shall, subject to the provisions of sub-section(3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.*

[415] The Information Technology Act, 2000, Section 48 states, *Establishment of Cyber Appellate Tribunal :*
(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal.
(2) The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

[416] Section 50 of Justice Srikrishna Committee Report.

prescribed by the Government[417], thus effectively compromising on the independence of this authority.

Thus, from the analysis of the above important components of data protection, the Researcher has observed that the proposed data protection legislation in India especially the Digital Personal Data Protection Bill, 2022 is prejudiced towards the entity collecting the data particularly the Government, and may have significant issues with the user's rights, this when internationally, data privacy laws have rightfully given users the major portion of collection and consent rights.

With the analysis and the authentication of the hypotheses, the Researcher advances to the conclusion, findings and suggestions in the subsequent chapter wherein the Researcher has highlighted the proposed provisions that form part of the Justice Srikrishna Committee Report, the PDP 2019, the JPC Report and the Digital Personal Data Protection Bill, 2022 in order to address some of the important issues undermining India's potentials of emerging as a secure destination for data protection.

[417] Section 19 of Digital Personal Data Protection Bill,2022

CHAPTER 6 – CONCLUSIONS, FINDINGS AND SUGGESTIONS.

6.1 INTRODUCTION :

The present modern day framework of communications and interactions is not limited to simply sharing information but transcends beyond into a digital realm with little or no legal implications and completely undermines an individual's privacy. The evolving contours of data transfers and transactions including cross - border data transfers have several legal and personal ramifications. Since the characteristics of the data being shared and transferred has transformed, and it may include a broad array of information, such as sensitive information, health records, financial data, biometric data, and defense-related information, among others, the transfer and sharing of such information may have serious legal ramifications. The implications of such sharing personal data on modern social media websites, Apps and communication systems are unidentified due to a variety of known and unknown factors, the advent of Artificial Intelligence and its unfathomed application has further impeded the need for protection of personal data.

While India presently lacks a robust and independent legislation for personal data protection, and as discussed in the preceding chapter the Government endeavoured and rose up to the occasion and formed the *Committee of Experts under the Chairmanship of Justice B.N.Srikrishna on A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians,2018* **("Justice Srikrishna Committee Report")** followed by the *Personal Data Protection Bill, 2019* **("PDP 2019")**, *the Report of the Joint Committee on The Personal Data Protection Bill 2019, 2021* **("JPC Report, 2021")** and has recently proposed *Digital Personal Data Protection Bill,2022* **("DPDPB 2022")** which awaits implementation .

In this chapter the Researcher essentially considers the important suggestions on data protection that form part of the Justice Srikrishna Committee Report, the PDP 2019, the JPC Report, 2021 and the proposed DPDPB, 2022 and makes a critical analysis of these proposed legislative frameworks and highlights the shortcomings therein while attempting to offer suggestions to have an enhanced, effective and robust data protection legislation for India.

6.2 CONCLUSIONS:

The present study is divided into six chapters that encompass various aspects of the data protection legal framework in the nations of the EU, the US, UK and in India. To arrive at a fair analysis of the research hypothesis, the Researcher has classified the chapters in a way that would enable for an optimised understanding of the significance of a strong personal data protection law in the country.

The most essential component of the study was to understand and analyse the existing law on information privacy in India and the proposed independent legislation on data protection in India, encompassing the Justice Srikrishna Committee Report, the PDP 2019, the JPC Report, 2021 and the proposed DPDPB, 2022, and thus arrive at a response to the thesis hypothesis.

As the title suggests, the thesis focused on comparing and analysing the legal frameworks regarding data protection in various jurisdictions EU, the US, UK and attempted an assessment of India's readiness in the sphere of data protection in light of emerging challenges in the digital and technological field.

It was alarming to note that India reported a total of 52,974 registered cases under Cyber Crimes, showing an increase of 5.9% in registration over 2020 (50,035 cases). Crime rate under this category increased from 3.7% in 2020 to 3.9% in 2021 and importantly during 2021, 60.8% of cyber-crime cases registered were for the

motive of fraud (32,230 out of 52,974 cases) followed by sexual exploitation with 8.6% (4,555 cases) and extortion with 5.4% (2,883 cases),[412] the proposed legislative framework including the proposed DPDPB, 2022 without a doubt, fall short of addressing some of the most critical issues concerning data protection in a free functioning democracy.

Following a comprehensive analysis of several of the key features of the data protection laws in the EU, the US, UK and the proposed data protection legislation for India, the Researcher has concluded that the research hypothesis is addressed in the affirmative, a conclusion that seemed to be evident from the discussions in all of the chapters.

The Researcher has nevertheless identified potential areas of research where there is scope for further research. The findings of the study and suggestions are discussed in detail herein under and the Researcher will in the following sections highlight the components of the proposed legislation that have made a significant contribution to the Researcher's conclusion regarding the hypothesis

6.3 FINDINGS :

The findings on the key areas of information privacy and data protection derived from the present study following the critical analysis of the Justice Srikrishna Committee Report, the PDP 2019, the JPC Report, 2021 and the proposed DPDPB, 2022 are discussed herein under:

[412] NATIONAL CRIME RECORDS BUREAU, MINISTRY OF HOME AFFAIRS, CRIME IN INDIA 2021, STATISTICS VOL-II, available at: https://ncrb.gov.in/sites/default/files/CII%202020%20Volume% 201.pdf (Last accessed on May 17, 2023). The report for the year 2022 is not available.

6.3.1 Findings derived from Critical Analysis of the Justice Srikrishna Committee Report:

The Justice Srikrishna Committee was set up to "study various issues regarding data protection in India", in the wake of the Supreme Court's ruling in the *Puttaswamy* case upholding the right to privacy as a fundamental right.

The draft Report provided that the Government, a private company, citizen, a person or a body of persons, who sought to process personal data needs was to do so in a "fair and reasonable" manner that safeguarded the individual's privacy. The Report also provided that only limited personal data could be collected, for a clear, specific and lawful purpose and individuals could be notified of the kind of data that had been collected. Barring certain situations, personal data could be collected and processed only with the explicit consent of the individual.

Importantly the Report exempted the State i.e. Government, from some of these obligations in two broad contexts. First were the situations where personal data needed to be processed (collected, stored, used, disclosed or shared) by the Government for one of the following reasons: (a).For the functioning of Parliament or State Legislatures, (b).For providing individuals with any service or benefit, (c).For issuing any certification, license or permit. In these situations, the Report listed certain other safeguards largely applicable, but exempted the Government from obtaining the consent of individuals before collecting or processing their personal data.

Secondly, the Report considered the situations where personal data was needed to be processed in the interest of the security of the country, or for prevention, detection, investigation and prosecution of any violation of law and allowed the Government wide exemption from the data protection law. It went on to recommend that the State enact a suitable law that would be applicable to intelligence or surveillance activities, provided that once such a law is enforced, all data processed for the purpose of the security of the State and law enforcement be exempted from

the data protection law. This thus gave rise to concerns of violation of personal information by the Government and its agencies.

In addition, the Report provided that some of the transparency and accountability measures laid out in the Report was only to be implemented by recognised *"significant data fiduciaries"*. Importantly the Report stated that the Data Protection Authority may or may not categorise Government agencies as *significant data fiduciaries*.

Further, the Committee's Report recognised that the relationship between and data principals and the State involved a power imbalance which was furthered as the State was not required to be accountable to its citizens, especially with regard to their personal data, thus, ironically setting a low bar for a personal data protection.

It can thus be argued that the Justice Srikrishna Committee Report though was a step forward with respect to protecting personal data rights in the country it was not close to the kind of reform that is needed to ensure that the right to privacy is protected adequately.

6.3.2 Findings derived from Critical Analysis of the PDP, 2019 :

Though the Personal Data Protection Bill, 2019 was based on the Report submitted by the Justice Srikrishna Committee, it did however make some of its own suggestions with the intention, to safeguard personal data, to secure additional rights for the data owner, ensure consent obtained was unbundled, clear, and received in real time and contained effective provisions on data localisation, however analysis of the PDP 2019, reveals that the Bill too fell short on the following grounds:

As was with the Justice Srikrishna Committee Report, the jurisdiction of this Bill was also vast in its applicability, and included both territorial and extraterritorial provisions along the lines of the EU GDPR. The Bill applied to both Governmental

and private actors as well as to any data processing done within India, as well as to any processing by the State, Indian companies or Indian citizens.

The Bill allowed the Central Government to specifically exempt any Government Agency from the provisions of the data protection law in the interest of sovereignty, integrity, public order, etc. and stated that exemption could be granted if the Government assessed that it was necessary, based on "subject to procedures", safeguards, and oversight systems to be stipulated by the Government. This effectively meant that the provision would give the Government unrestricted powers to exempt any Government Agency from the applicability of the data protection law itself.

The Bill also laid down the grounds on which the Government could process personal data without the *consent* of the individual. This was perilous as it diluted the importance of *consent* of the individual and allowed the Government to process personal data without individual's consent in order to provide a service or benefit to the individual.

In furtherance to the RBI requirements for payment companies to store data in India, data localisation rules suggested by this Bill emphasised that one copy of all personal data to which the data protection law applied were to be kept in a server within India. Further, it provided that certain categories of data, which were to be specified by the Government as *critical personal data* were mandatorily to be stored in India alone.

The Bill created several exceptions and exemptions for processing of data by the State and apart from the grounds recommended by the Justice Srikrishna Committee included additional grounds for processing data under Section 13 (Chapter III) where processing of data was required for the *"function of the State (authorised by the law), Parliament, or the Legislature"*. This thus included processing of personal data for the provision of any service or benefit to the data principal from the State.

The Bill further proposed for the establishment of a *Data Protection Authority* **("DPA")**, which was to function as an independent regulator for data protection. However the Bill conferred on the Government the power to appoint the Chairman and the Members of the DPA, which effectively took away the independence of the DPA which becomes paramount especially in situations where the Government itself assumed the role of data fiduciary and engaged in collection of individual's personal data.

The Bill sought to dilute the powers of the DPA by conferring certain proposed original powers and functions of the DPA onto the Central Government, for example: (a). Under the Justice Srikrishna Committee Report, the DPA was given the authority to notify additional categories of *sensitive personal data* however the PDP, 2019 Bill conferred this power only onto the Government, in consultation with the sectoral regulatory authorities (b).Under the Justice Srikrishna Committee Report, the DPA had sole authority to identify and notify *significant data fiduciaries*, however, in terms of the PDP, 2019 Bill, the Central Government, in consultation with the DPA, was conferred with this power.

The PDP, 2019 Bill required *non-personal data* collected and developed privately to be shared with the Government. The Bill however conferred unfettered powers on the Government to direct any data fiduciary or data processor to provide to it any *anonymized personal data* or other *non-personal* data to enable the Government to better target service delivery or formulate evidence-based policies.[413]

This was distressing as it was incomprehensible as to why a personal data protection law would engage with *non-personal* data at all. Further, the Bill did not specify how the Government would use such data, and whether organisations obligated to share such data would be reimbursed. As a result, the Government

[413] The Personal Data Protection Bill, 2019, Section 91 (2) states:- *The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed.*

would have got the authority to expropriate the intellectual property of the organisation, which was likely to have a negative impact on the incentives for innovation to the organisation in the long term.

The Bill required that *data breach notifications* to be made to the DPA by the data fiduciary if the breach was likely to cause harm to the data principal, it thus left this discretion not on the data principal but on the data fiduciary who was to judge if the data breach caused harm to the data principal or not, which was a matter of deep concern.

The Bill prescribed steep penalties including penalties higher than INR 5 Cr or 2% of annual global turnover of the company in question for violations like failing to conduct a data protection audit. A penalty of higher than INR 15 Cr or 4% of the annual global turnover of the company in question was prescribed for violations such as processing of personal data in contravention of the Bill. It provided that complaints could be filed by an aggrieved *data principal* to *adjudicating officers* who were to be appointed under the Bill and that Appeals from their orders would be to an Appellate Tribunal and thereafter to the Supreme Court. The Bill also prescribed a list of non-bailable and cognizable criminal offences, which included a maximum fine of INR 2 Lakh or imprisonment of three years for obtaining, transferring, or selling personal data in violation of the law.

Thus, on critically analysing the Bill, it can be inferred that the broad powers proposed to be conferred on the Government by the PDP, 2019 Bill raised the possibility of the Government engaging in mass surveillance, which infringed the fundamental Right to Privacy. Apart from this, the PDP, 2019 Bill also failed to qualify the three pronged test of *'legality'*, *'need'*, and *'proportionality'* for identifying violations of the constitutional right of privacy in more than one way.

6.3.3 Findings derived from Critical Analysis of the JPC Report, 2021 :

The PDP, 2019 Bill due to its shortcomings, was referred to a *Joint Parliamentary Committee* **("JPC")** which comprised of members of both houses of Parliament (of India). The JPC's Report, was incorporated as a new version of the PDP 2019 and was referred to as *the Report of the Joint Committee on The Personal Data Protection Bill 2019, 2021* **("JPC Report, 2021"),** though it retained the majority of the provisions from the PDP, 2019 Bill it suggested amendments to the same and also added certain new provisions. However an analysis of the JPC Report 2021 reveals that it also falls short on the following grounds:

The very preamble of the JPC Report, 2021 was one of the first noticeable changes, which included the terminology "*to ensure the interest and security of the State*" in the opening paragraph of the preamble, by which the JPC Report, 2021 at the very outset diminished the primacy of an individual's privacy. This clearly indicated that the proposed law's primary goal was to serve security interests of the State which clearly was misplaced within a data protection law.

Further, The JPC Report, 2021 changed the name of the law from "***Personal Data Protection Bill***" to "***The Data Protection Bill, 2021***." This was due to the draft law's expanded regulatory scope, which was intended to also administer *"non-personal data"*. The premise failed to convey the complexities of *non-personal data*, considering that *non-personal data* is frequently *de-anonymised*, and could affect personal data of an individual even when aggregated and non-identifiable through the available and evolving digital systems.

Consent is the fundamental framework of any data protection law. This necessitates the need for the individual to be put on notice and provide the individual the opportunity to exercise his or her consent. However the JPC Report, 2021 eliminated the additional safeguards of "legitimate purpose" and "proportionality," and infact widened the exemption for seeking consent. Further, it included "quasi-

judicial authorities" as agencies with the authority to process personal data without consent. It infact facilitated *non-consensual processing* when it could reasonably be expected by the data principal, this predominantly undermined the principle of "*express consent*" as would be in the case of employees, as they would not have to be specifically informed when their personal data was processed by the employer.

Users were provided certain rights under the JPC Report, 2021 including the *right to confirmation and access*, *right to correction and erasure*, *right to data portability*, and the *right to be forgotten*. The treatment of the *right to be forgotten* was noteworthy since the JPC Report, 2021 itself granted an exemption from its application for "*the data fiduciary's right to retain, use, and process such data*". This made little sense, for the reason that, data principals have *legal rights* and data fiduciaries that process their data have *legal duties and responsibilities*. The effect of such a change is that it tends to increase the discretion of Government agencies and organisations being the data fiduciaries to retain personal data of the data subjects.

The JPC Report, 2021 however acknowledged the "*increasing importance of data localisation*", as in addition to maintaining clauses regarding data localisation, it called on the Government to "*prepare and pronounce an extensive policy on data localisation*". It further provided for significant changes that enlarged the grounds for prohibiting transfers of *sensitive and critical personal data* when the object of such transfer was against public policy or State policy. Interestingly however, the terms "*public policy*" and "*State policy*" remained undefined in the JPC Report, 2021, which could have potentially lead to ambiguity and unguided discretion for the Data Protection Authority to enforce.

The JPC Report, 2021 ironically, made it simpler for the Government to evade the jurisdiction of a data protection law entirely as it solidified the exemption for Government Entities by inserting a provision in Clause 35 that read, "*Notwithstanding anything contained in any law currently in force* ". In addition,

explanation (iii) to Clause 35 of the JPC Report, 2021 referred to safeguards that were to be in accordance with a "*just, fair, reasonable, and proportionate procedure*". It is important to emphasise here that these exemptions could have been applied to instances of interception and mass surveillance technologies including facial recognition, which were not covered by the proposed Data Protection law or any other current legislative proposal from the Central Government.

The Data Protection Authority, should be an independent, autonomous, and well-resourced regulatory body, responsible for enforcing data protection rights, however, the JPC Report, 2021 provided for the appointment and authority of the Data Protection Authority to be structured in a way that gave the Government complete control and authority over it, as the *Selection Committee* for appointing members of the Data Protection Authority were to be comprised entirely of executive members. This would undoubtedly imply that the Data Protection Authority would be disposed to the Government.

While the JPC Report, 2021 suggested certain modifications to the selection and appointment of the members of the Selection Committee from that proposed in the PDP, 2019 Bill, through which the Attorney General, an independent expert, a director of an IIT, as well as a director of an IIM found place in the selection panel, the fundamental issue of independence of the Data Protection Authority yet remained debatable, as all such appointments were made at the discretion of the Government. Furthermore, the JPC Report, 2021 suggested that the Data Protection Authority be bound by the directions of the Government in all cases, not just on questions of policy. As a result, the Government's decision would be final in all matters, thereby entirely wearing down the independence of the Data Protection Authority.

Thus on analysing the provisions of the JPC Report, 2021 it can be inferred that the JPC Report’s recommendations deviated from the framework of the PDP Bill, 2019,

as the JPC Report, 2021 was prone to be misapplied by the State, jeopardizing people's fundamental rights. Moreso as its is the privacy and data protection that must assume primacy in the digital era, and both must be protected to the same degree and extent, and thus considering the shortcomings, the Government on August 03, 2022 withdrew the said JPC Report, 2021 and replaced it with a new Bill which was to be a 'comprehensive framework' and contain 'contemporary digital privacy laws'.[414]

6.3.4 Findings derived from Critical Analysis of the DPDPB, 2022 :

The Ministry of Electronics and Information Technology introduced the draft *Digital Personal Data Protection Bill, 2022* **("DPDPB, 2022")** as the legislation for digital data protection in the country. Interestingly, the DPDPB, 2022, contains approximately no more than 30 clauses, which is a significant reduction from previous data protection legislation proposals, which were exhaustive. The analysis of the DPDPB, 2022 reveals the following:

The most concerning issue with DPDPB, 2022 is the fact that its provisions cover a basic framework for data protection and privacy, leaving it largely for the Central Government to assess and notify further protections at a later stage, as and when deemed necessary. This not only puts the ambit of Governmental scrutiny at a wider reach but also prevents adequate protection of fundamental right to privacy.

The DPDPB, 2022 continues with the broad and ambiguous exemptions granted to the Government in the JPC Report, 2021. Infact clause 18(2)(a) of the DPDPB[415], 2022, in particular, replicates Clause 35 of the JPC Report, 2021[416] and permits the Government to exclude any "*instrumentality*" of the Government from the very

[414] Govt withdraws Data Protection Bill, 2021, will present new legislation, Business Standard, available at: https://www.business-standard.com/article/economy-policy/centre-withdraws-personal-data-protection-bill-2019-to-present-new-bill-122080301226_1.html (Last accessed on August 13, 2022).

[415] Digital Personal Data Protection Bill,2022, Section 18(2)(a) states:-*The Central Government may, by notification, exempt from the application of provisions of this Act, the processing of personal data:*
a. by any instrumentality of the State in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these.

[416] Recommendation No.56 of the JPC Report, 2021.

application of the DPDPB, 2022 in the interests of "*sovereignty and integrity, security, friendly relations with foreign States, maintenance of public order, or deterring incitement to any cognizable offence pertaining to any of these*". This would provide immunity to the notified Government entities from the application of the law, potentially leading to massive infringements of citizen's privacy.

It further provides that, *Consent* of a Data Principal for data processing will be *"deemed"* under certain circumstances, including the maintenance of public order, employment-related purposes, and in the public interest. These categories could permit broad and ambiguous interpretations of *"when"* a Data Principal is deemed to have given consent, thus enabling for increased processing of personal data acquired in the absence of clear, specific and informed consent

The DPDPB, 2022 proposes the establishment of a *Data Protection Board of India*, instead of a Data Protection Authority. It further provides that the Board's composition, the procedure and process of selection, the conditions and terms of appointment and service, and the removal of its Chairperson and other Members will be stipulated by the Government at a later stage. It further also states that, the Government would also appoint the Board's Chief Executive.
These provisions reflect the similar provisions contained in the JPC Report, 2021, as the now proposed *Data Protection Board* also appears to lack the independence required to adequately safeguard the interests of Data Principals. Moreso as the *Data Protection Board* is responsible for ensuring that the provisions of the legislation are followed by both the private sector and Government entities, it thus becomes all the more imperative that the proposed Data Protection Board be inherently independent of any Government control.

The DPDPB, 2022 requires the *Data Fiduciaries* to simply notify the *Data Principal* about the nature of data they will collect and the purpose for which such data may be processed. Unlike previous versions of the Bill, it does not require *Data Fiduciaries* to notify the *Data Principal* about the third parties to whom their

data will be shared, the amount of time their data will be stored for, as well as whether or not their data will be transferred to other countries. As a result, *Data Fiduciaries* can continue to obtain the *Data Principal's* consent by presenting limited information and then using their personal data in ways that the *Data Principal may* not have contemplated.

The DPDPB, 2022 provides *Data Principals* the *right to information* about personal data, the *right to correction and erasure*, the *right to redressal of grievances*, and the *right to nominate*. It does, however, impose certain obligations and penalties on them and includes complying with all applicable laws, not filing a false or frivolous grievance or complaint with a *Data Fiduciary* or the *Data Protection Board*, not providing any false particulars, suppressing any significant information, or impersonating another person, and providing only irrefutably authentic information. Non-adherence with these provisions may result in a fine of up to Rs.10,000/- being imposed, this is concerning since the law that is intended to protect individuals rights is now seeking to impose penalties on them.

Further, the term *"as may be prescribed"* is repeated significantly in the DPDPB, 2022. This indicates of the Government's ambiguous intent and unchecked powers to frame rules at a later point in time in the absence of legislative guidance.

The DPDPB, 2022 Bill also no longer requires *data localisation*, enabling tech giants to transfer personal data to specific countries and territories even outside the borders of India to certain countries as the Government may stipulate, indicating that though data transfer to any other country is precluded unless determined by the Government, it however does not specify any criteria or standards for the Government to consider when determining which countries to permit data transfers to.

This could therefore allow for the power to be exercised arbitrarily by the Government with countries selected or not selected based on criteria that go beyond

the protection of Indian citizen's personal data. Interestingly, this stands also in contrast to Articles 44 to 50 of the EU GDPR, which allow European's personal data to be transferred only to countries that provide a reasonable level of protection to this data i.e based on the *adequacy decision*.

The DPDPB, 2022 recommends to amend the Right to Information Act of 2005, specifically Section 8 (1)(j) [417] of the RTI Act that would wholly exempt "*personal Information*" from being disclosed. The suggested amendment intends to do away with the exceptions carved out within the Section 8 (1)(j) of the RTI Act based on which even personal information could have been disclosed. Currently, in order to deny personal information, at least one of the following grounds has to be proven – information sought has no relationship to any public activity, or information sought has no relationship to any public interest, or information sought would cause an unwarranted invasion of privacy and PIO/appellate authority is satisfied that there is no larger public interest that justifies disclosure. The suggested amendment will however wholly exempt any disclosure of personal information thereby diluting the effect of the RTI Act.

On the positive note, the earlier versions of the data protection legislation had a serious flaw, in that, they did not require *Data Fiduciaries* to inform *Data Principals* in the event of a data breach. As a result, users whose data has been compromised had no idea that their data had been compromised. The DPDPB, 2022 however attempts to address this concern by requiring *Data Fiduciaries* to inform the *Data Protection Board* and *Data Principals* of any breach, regardless of its nature. It then authorises the Board to direct the *Data Fiduciary* to take immediate

---

[417] The Right to Information Act, 2005, Section 8(1)(j) states:- *Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen-*
(j) information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information:
Provided that the information which cannot be denied to the Parliament or a State Legislature shall not be denied to any person.

action to redress any personal data breach or mitigate any harm caused to *Data Principals*.

Though this is encouraged, it is envisaged that this could create a conflict between the *Data Protection Board's* role and that of the *Computer Emergency Response Team* **("CERT")** which is presently tasked with responding to data breaches in the country.

A further positive aspect of the DPDPB, 2022 is that, significant barriers to the processing of *children's personal data* have been placed. It precludes *Data Fiduciaries* from tracking or monitoring children's behaviour, as well as targeting advertising to children. Though this provision is encouraged, the DPDPB, 2022 confers on the Government the prerogative to exempt *Data Fiduciaries* from these obligations. Further, the DPDPB, 2022 includes no mention of the standards or criteria that the Government would use to grant such an exemption.

The DPDPB, 2022 also proposes severe penalties for businesses that incur data breaches or fail to notify users when breaches occur. It provides that entities who fail to implement *"reasonable security safeguards"* to prevent personal data breaches may face penalties of up to Rs. 250 Cr which can exceed to Rs.500 Cr.

Thus, from the analysis mentioned above it can be inferred that although DPDPB, 2022 attempts to establish a comprehensive legislative framework governing digital personal data protection in India, by requiring the processing of digital personal data in a way that recognises individuals' right to safeguard their personal data, societal rights, and the necessity to process personal data for legitimate purposes, the DPDPB, 2022 is vaguely worded and fails to adequately clarify a number of important aspects of data protection in an effort to condense the earlier text. Thus while the PDP, 2019 delve into each aspect at a very exhaustive level, the DPDPB,2022 has left most aspects for subordination legislation (i.e. providing more powers to the Government to frame rules and regulations later) and the

Researcher therefore intends to make certain suggestions that will make the DPDPB, 2022 more effective and robust.

6.4 SUGGESTIONS:

The analysis undertaken by the Researcher reveals that the earlier proposals of the data protection law and the now proposed the DPDPB, 2022 do have shortcomings and hence the Researcher, with the intention to provide effectiveness and efficiency to the data protection legislation proposes to make the following suggestions to the DPDPB, 2022:

i. The DPDPB, 2022 presently covers only *digital personal data*, and as such it is suggested that it should include in its ambit *personal data* as well as *non-personal data (i.e.* data which does not contain personally identifiable information) as *non-personal data* can be used to map consumer biases, consumer preferences etc, or such other purposes and non-inclusion of such *non-personal data* from the purview of the data protection law can leave scope for violation .

ii. The DPDPB, 2022 is intended to apply to *digital personal data* however it is noted that there is no explicit definition of the term *"digital"***.** It is also unclear if the Bill will apply to mechanical and semi-automated data processing. Thus it is suggested that a clear definition of the term *"digital"* be included in the Bill to avoid ambiguity.

iii. The DPDPB, 2022 confers on the Data Principal the *right to withdraw their consent* at any time, and if done so, the Bill provides that the Data Fiduciary is responsible to cease processing the *personal data* of the Data Principal. However, it is observed that no time limit is mentioned in this Bill for the Data Fiduciary to cease the processing. It is therefore suggested that a clear time limit

be stated in the Bill for the Data Fiduciary to cease the processing, so as avoid delays and continuance of processing of the data even after the withdrawal of consent by the Data Principal.

iv. The DPDPB, 2022 provides for the concept of *Deemed Consent***,** in which the Data Principal is *deemed* to have given consent to the processing of their personal data, if such processing is necessary in requirements like public interest, issuance of certificate under law, compliance with any judgment or order by law, medical treatment during epidemic or other disasters, employment, credit scoring, recovery of debt, operation of search engines of publicly available personal data etc. It is observed that there is a wide area of ambiguity here as any number of data processing scenarios could fall under the *deemed consent* sphere of the law. Further, the Bill also does not clarify whether *deemed consent* can be *withdrawn* by the Data Principal, and what would be the procedure for such withdrawal. It is thus suggested that the Bill includes express provisions pertaining to *deemed consent* to prevent its misuse.

v. The DPDPB, 2022 makes that Data Fiduciary responsible for implementing appropriate technical & organisational controls to protect personal data collected and states that reasonable security safeguards are to be implemented to prevent data breach. It further provides that the Data Fiduciary is required to notify the *Data Protection Board of India* and each affected Data Principal in the event of a data breach. It is however observed that, there is no time duration specified in the DPDPB, 2022 for such notification. It is therefore suggested that a clear time limit be stated in the Bill so as avoid delays.

vi. The age when a person is considered capable of consenting in the online world is linked to the age of consent under the Indian Contract Act, that is 18 years and the DPDPB, 2022 also considers the same. It is observed that there is no distinction made between a 5-year-old and a 17-year-old in the DPDPB, 2022. As a consequence, it assumes that all people under 18 years of age have the

same maturity level. Moreover, classifying all people under the age of 18 years as children disregards how young adults and teenagers use the internet. It is therefore suggested that instead of establishing a blanket age for deciding valid consent i.e. 18- years, alternative methods for determining the appropriate age for children at various ages of maturity may be considered, similar to the *Age Appropriate Code 2021*[418] developed by the UK Information Commissioner's Office which prescribes 15 standards that online services need to adhere to when considering an individual capable of consenting.

vii. The DPDPB, 2022 provides for *data transfer*, as Data Fiduciaries can now transfer *personal data* to certain countries as the Government may stipulate, indicating that *data transfer* to any other country is precluded (and hence indirectly also provides for *data localisation*). It is however observed that the DPDPB, 2022 does not specify any criteria or standards for the Government to consider when determining which countries to permit data transfers to. It is therefore suggested that criteria or standards for the Government to consider when determining which countries to permit data transfers be incorporated in the DPDPB, 2022 as this will bring about certainty and prevent arbitrarily exercise of this power by the Government with countries selected or not selected based on criteria or factors that go beyond the protection of Indian citizens' personal data.

viii. The DPDPB, 2022 grants the Government the authority to exempt any Government Agency from the full application of this law, even if it is merely in the interest of "public order". Further, it gives blanket authority to the Government to exempt certain Data Fiduciaries or class of Data Fiduciaries from the application of this law. It is observed that this grants a *carte blanche* to the Government from the full application of this law more-so when the Government is one of the biggest *data processor*. It is therefore suggested that

---

[418] Age appropriate design: a code of practice for online services, available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf (Last accessed on November 15, 2022).

the use of data by the Government and its agencies must be monitored and that the DPDPB, 2022 should limit the amount of data collected by law Government agencies especially enforcement agencies, and also necessitate the Government agencies to implement security measures to protect the personal data.

ix. An independent and robust *Data Protection Authority* is the cornerstone of a strong data protection regime. The DPDPB, 2022 proposes the establishment of a *Data Protection Board of India*, rather than a *Data Protection Authority*, which is tasked with grievance redressal and compliance of the provisions of this law. It provides that the Board's composition, the procedure and process of selection, the conditions and terms of appointment and service, and the removal of its Chairperson and other Members shall be as stipulated by the Government at a later stage. It further states that, the Government would also appoint the Board's Chief Executive. It is observed that this causes concerns about the independence of such a body. Given that the Government is one of the biggest collector of personal data over which the Board will have jurisdiction, ensuring its independence is absolutely essential. It is therefore suggested that to minimise executive control, the appointment process of the Board must be transparent and devoid of Government interference. Also the law should provide fort establishment of a substantial Board that is well-funded, has sufficient personnel, and has offices atleast in major parts of India. This will make the Board accessible to citizens throughout the country and prove effective in grievance redressal.

x. Last but not the least, it is strongly suggested that only after comprehensive public consultation should the new data protection legal framework be implemented. This will help make sure of the protection of Indian citizen’s right of privacy.

The DPDPB, 2022 considered and analysed in the present study is the most recent Bill proposed by the Government on Digital Personal Data Protection, however, the

Bill is still under consideration of the Parliament of India and has not yet been enacted.

The present study had limitations of time and other predicaments as discussed earlier and it is only after the Bill is implemented that we will be in a position to analyse the extent to which the phenomenon of Digital Personal Data Protection is positively addressed.

The Government nevertheless has to work out the modalities for executing the provisions and overcome the practical challenges that may come its way and thus, there is a scope for advancing and delving further on this research subject.

BIBLIOGRAPHY

BOOKS

ALAN F. WESTIN, PRIVACY AND FREEDOM, 25 WASH. & LEE L. REV. 166 (1968).

DHIRAJ R. DURAISWAMI, PRIVACY AND DATA PROTECTION IN INDIA, J.L. & Cyber Warfare 166, 169-72 (2017).

HELEN NISSENBAUM, PRIVACY IN CONTEXT-TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE, Stanford University Press, 2010.

JERRY KANG, INFORMATION PRIVACY IN CYBERSPACE TRANSACTIONS, Stanford Law Review, April 1998.

JOEL REIDENBERG, RESOLVING CONFLICTING INTERNATIONAL DATA PRIVACY RULES IN CYBERSPACE, Stanford Law Review 1999.

LEE BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC, AND LIMITS, Kluwer Law International, 2002.

PAWAN DUGGAL, DATA PROTECTION LAW IN INDIA, Universal Law Publishing, First Edition, 2016.

ROBERT HASTY, DR. TREVOR W. NAGEL AND MARIAM SUBJALLY WHITE AND CASE, DATA PROTECTION LAW IN THE USA, Advocates for International Development, August 2013.

ARTICLES

Arushi Chopra, *Number of Internet users in India could cross 450 million by June*: http://www.livemint.com/Industry/QWzIOYEsfQJknXhC).

Ashwini Siwal , *A Comparative Analysis of The Legal Framework Related to Data Protection In India, U.S.A. & U.K. with Special Reference to Inter - Country Problem of Outsourcing***,** submitted to Jamia Millia Islamia (http://shodhganga inflibnet.ac.in/hdl.handle.net/10603/307411).

Bhumesh Verma and Ujjwal Agrawal, *Evolution of Data Privacy*, Sayantan Dey Legal and Compliance Professional (https://www.scconline.com/blog/ post/2020/02/06/evolution-of-data-rivacy/#:~:text=Privacy%20was%20 statutorily%20recognised%20globally,provisions%20in%20their%20domestic%20laws).

Bruce Schneier, *Why anonymous data sometimes isn't, Wired* (December 12, 2017), (https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/)

Deb Miller Landau, *Artificial Intelligence and Machine Learning: How Computers Learn, IQ Intel* (August 17, 2016), (https://iq.intel.com/artificial-intelligence-and-machine-learning/).

Economic Laws Practice, *Data Protection & Privacy Issues in India.EMC Digital Universe with Research and Analysis by IDC, The Digital Universe of Opportunities: Rich Data and the Increasing Values of the Internet of Thing*s, (April,2014),(https://www.emc.com/leadership/digital-universe/2014iview/ executive-summary.htm).

European Commission, Data Protection Working Party Opinion, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, (September 16, 2014),

(http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf).

IBM, *10 Key Marketing Trends for 2017 and Ideas for Exceeding Customer Expectations (*https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?Htmlfid =WRL12345USEN)

Information Commissioner‘s Office (UK), *Big Data, Artificial Intelligence, Machine Learning and Data Protection* (https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/).

Jordi Soria-Comas and Josep Domingo-Ferrer, Big Data Privacy: *Challenges to Privacy Principles and Models, 1(1) Data Science and Engineering* (March, 2016) (available at: https://link.springer.com/article/10.1007/s41019-015-0001-x).

Pam Dixon, *A Brief Introduction to Fair Information Practice Principles, World Privacy Forum* (2006) (https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information- practices).

Pooja Kiwayat, *Data Protection Law in India A comparative Study of existing data protection regime with reference to EU UK USA*, submitted to Jagran Lakecity University (http://shodhganga inflibnet.ac.in/hdl.handle.net/10603/362372).

Press Information Bureau, *Home Minister Proposes Radical Restructuring of Security Architecture*, Ministry of Home Affairs, Government of India (December 23, 2009) (http://pib.nic.in/newsite/erelease.aspx?relid=56395).

Ranjan Guha, *Digital Evolution in India* (http://www.businesstoday.in/opinion/columns/digital-evolution-in-india /story/259227.html)

Roger Parloff, *Why Deep Learning is Suddenly Changing your Life*, Fortune Magazine (September 28,2016) (http://fortune.com/ai-artificial-intelligence-deep-machine-learning/).

Samuel Warren and Louis Brandeis, *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5, Dec. 15, 1890 (https://www.jstor.org/stable/1321160).

Shivani Joshi, *Data Protection In India : A Comparitive Study* (http://shodhganga inflibnet.ac.in/hdl.handle.net/10603/385428).

Sian Rudgard, *A Race for Maintaining Personal Data - How to Manage Consumers' data under the Right to Be Forgotten and the Right to Data Portability of the new EU GDPR* (https://run.unl.pt/bitstream/10362/38767/1/ Vale_2018.pdf).

Sian Rudgard, *Origins and Historical Context of Data Protection Law* (https://www.scribd.com/document/435237603/European-Privacy-Chapter-One).

Stephen J. *Bigelow, Data Privacy (Information Privacy)* (https://www.techtarget.com/searchcio/ definition/data-privacy-information-privacy

The Society for the Study of Artificial Intelligence and Simulation of Behaviour, *What is Artificial Intelligence* (http://www.aisb.org.uk/public-engagement/what-is-ai).

STATUTES, MANUALS AND SCHEME

Aadhaar (Data Security) Regulations, 2016.

Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.

California Civil Code §§ 1798.83.

California Consumer Privacy Act 2018.

California Financial Information Privacy Act, 2004.

California Online Privacy Protection Act, 2004.

California Shine the Light Law, 2003.

Charter of Fundamental Rights of The European Union.

Charter of Fundamental Rights Of The European Union (2000/C 364/01).

Children's Online Privacy Protection Act, 2000.

Clinical Establishments (Central Government) Rules, 2012.

Code of Bank‘s Commitment to Customers, Privacy and Confidentiality, Banking Codes and Standards Board of India (June 2014).

Colorado Privacy Act, 2023.

Computer Fraud and Abuse Act, 1986.

Connecticut Personal Data Privacy and Online Monitoring Act, 2023.

Constitution of India, 1950.

Controlling the Assault of Non Solicited Pornography and Marketing Act of 2003.

Convention for the Protection of Human Rights and Fundamental Freedoms

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,1981.

Council of Europe Convention for the Protection of Individuals Regarding Automatic Processing of Personal Data.

Council of Europe Recommendations, 1968.

Credit Information Companies (Regulation) Act, 2005.

Credit Information Companies Regulation, 2006.

Criminal Procedure (Identification) Act, 2022.

Data Protection Act 1984.

Data Protection Act, 1998.

Data Protection Act,2018.

Digital Personal Data Protection Bill, 2022.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

Electronic Communications Privacy Act, 1986.

EU General Data Protection Regulation, 2016.

Fair and Accurate Credit Transactions Act, 15 U.S.C. §§ 1681-1681x.

Fair Credit Reporting Act, 1970.

Fair Information Practices Principles.

Family Educational Rights and Privacy Act,1974.

Federal Trade Commission Act, 1994.

Federal Trade Commission Enforcement of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks.

Gramm-Leach-Bliley Act, 1999.

Gramm-Leach-Bliley Safeguards Rule,2021.

Health Insurance Portability and Accountability Act,1996.

Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations, 2002.

Indian Telegraph Act, 1885.

Indian Wireless Telegraphy Act, 1933.

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Information Technology Act, 2000 (as amended by the Information Technology Amendment Act, 2008.

Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015.

Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017.

Insurance Regulatory and Development Authority of India (Sharing of Database for Distribution of Insurance Products) Regulations, 2010.

International Covenant on Civil and Political Rights

Massachusetts Data Privacy Law, 2009.

Mental Healthcare Act, 2017.

New York Privacy Act, 2021.

Non-Solicited Pornography and Marketing Act, 2003.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data , 2013.

Ohio Data Protection Act, 2018.

Organisation for Economic Co-operation and Development, Thirty Years After: The OECD Privacy Guidelines, 2011.

Personal Data Protection Bill, 2019.

Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983.

RBI Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card Operations of Banks and Credit Card issuing NBFCs

RBI Master Circular on Credit Card, Debit Card and Rupee Denominated Cobranded Prepaid Card operations of banks dated 1 July 2014.

RBI Master Circular on Customer Service in Banks, 2015.

RBI Master Circular on Customer Service in UCBs ,2015.

RBI Master Direction on Know Your Customer (KYC) Direction 2016.

Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016

Reserve Bank of India's Directive 2017-18/153 (April 6, 2018)

Reserve Bank of India's Directive 2017-18/153 (April 6, 2018),

Right to Information Act, 2005

Telecom Commercial Communications Customer Preference Regulations, 2010.

Telecom Regulatory Authority of India Act, 1997.

Telephone Consumer Protection Act, 1991.

Treaty on the Functioning of the European Union

Treaty on the Functioning of the European Union.

U.S.-EU Safe Harbor Frameworks.

UN General Assembly Resolution On The Right To Privacy In The Digital Age, A/RES/68/167, New York, 18 December 2013.

UN General Assembly, Revised Draft Resolution On The Right To Privacy In The Digital Age, A/C.3/71/L.39/ Rev.1, New York, 16 November 2016.

UN General Assembly Revised Draft Resolution On The Right To Privacy In The Digital Age, A/C.3/69/L.26/Rev.1, New York, 19 November 2014.

United States Privacy Act, 1974.

Universal Declaration of Human Rights

Video Privacy Protection Act , 1988.

Virginia Consumer Data Protection Act, 2021.

REPORTS

EUROPEAN COMMISSION, EUROPEAN DATA PROTECTION REFORM AND BIG DATA: FACTSHEET, (2016).

HANDBOOK ON EUROPEAN DATA PROTECTION LAW, 2018

INFORMATION COMMISSIONER‘S OFFICE (UK), BIG DATA, ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND DATA PROTECTION.

JUSTICE B.N.SRIKRISHNA COMMISSION, WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA.

KRISHNA MENON, ANALYSIS OF THE REPORT ON THE DATA PROTECTION BILL, 2021 BY THE JOINT PARLIAMENTARY COMMITTEE.

LINDOP REPORT ON DATA PROTECTION (1974)

LINDOP REPORT ON DATA PROTECTION (1978)

NATIONAL CRIME RECORDS BUREAU, MINISTRY OF HOME AFFAIRS, CRIME IN INDIA 2021, STATISTICS Vol-II,

REPORT ON PRIVACY, SECURITY AND OWNERSHIP OF THE DATA IN THE TELECOM SECTOR, TELECOM REGULATORY AUTHORITY OF INDIA , 16th July 2018.

THE EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), THE COUNCIL OF EUROPE AND THE REGISTRY OF THE EUROPEAN COURT OF HUMAN RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW (2014).

THE EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), THE COUNCIL OF EUROPE AND THE REGISTRY OF THE EUROPEAN COURT OF HUMAN RIGHTS, HANDBOOK ON EUROPEAN DATA PROTECTION LAW (2014)

YOUNGER REPORT ON PRIVACY (1972)

NEWSPAPERS

THE ECONOMIC TIMES

THE TIMES OF INDIA, March 20,2017

THE INDIAN EXPRESS, November 20, 2017

THE INDIAN EXPRESS, March 02, 2018

THE INDIAN EXPRESS, March 11, 2018

THE INDIAN EXPRESS, March 26, 2018

THE INDIAN EXPRESS, May 15, 2019

THE INDIAN EXPRESS, October 31, 2019

THE INDIAN EXPRESS, March 27, 2022.

WEBLIOGRAPHY

www. conventions.coe.int

www.artsandculture.google.com

www.assembly.coe.in

www.assembly.coe.int

www.bcs.org

www.bitraser.com

www.bja.ojp.gov

www.brainyquote.com

www.business-standard.com

www.business-standard.com

www.centraleyes.com

www.codes.findlaw.com

www.compliancy-group.com

www.congress.gov

www.consumercal.org

www.consumercal.org

www.cookiebot.com

www.csoonline.com

www.dataprotection.ie

www.dataprotection.ie

www.dbs.com

www.dla.gov.in

www.donotsell.org

www.dot.gov.in

www.ec.europa.eu

www.ec.europa.eu

www.echr.coe.int

www.economictimes.indiatimes.com

www.elplaw.in

www.emc.com

www.eur-lex.europa.eu

www.eur-lex.europa.eu

www.fpc.gov

www.fra.europa.eu

www.ftc.gov

www.ftc.gov

www.gdpr.eu

www.gov.uk

www.govinfo.gov

www.govinfo.gov

www.helpy.io

www.hudoc.echr.coe.int

www.hutchlaw.com

www.ico.org.uk

www.indiatvnews.com

www.kirkpatrickprice.com

www.law.lis.virginia.gov

www.leg.colorado.gov

www.legislation.gov.uk

www.legislation.gov.uk

www.livemint.com

www.mass.gov

www.medium.com

www.meity.gov.in

www.merriam-webster.com

www.nacdl.org

www.ncbi.nlm.nih.gov

www.ncrb.gov.in

www.ncrb.gov.in

www.nibusinessinfo.co.uk

www.oag.ca.gov

www.ohiobar.org

www.pib.nic.in

www.portal.ct.gov

www.privo.com

www.rbi.org.in

www.rm.coe.int

www.scconline.com

www.sflc.in

www.shodhganga inflibnet.ac.in

www.techtarget.com

www.trai.gov.in

www.ucl.ac.uk

www.ucl.ac.uk

www.un.org

www.uscode.house.gov

www.varonis.com