



**A CRITICAL LEGAL STUDY ON DATA PROTECTION LAWS
IN INDIA AND ITS APPLICABILITY IN THE STATE OF
NAGALAND**

**THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE
REQUIREMENTS FOR THE DEGREE OF DOCTOR OF
PHILOSOPHY**

**By
Ms. SONIA NATH
Ph D. REGN NO: PHD/LAW/00705**

**DEPARTMENT OF LAW
SCHOOL OF SOCIAL SCIENCES
NAGALAND UNIVERSITY, LUMAMI**

APRIL 2026

**A CRITICAL LEGAL STUDY ON DATA PROTECTION LAWS
IN INDIA AND ITS APPLICABILITY IN THE STATE OF
NAGALAND**

BY

**Ms. SONIA NATH
Ph D. REGN NO: PHD/LAW/00705**

NAME OF SUPERVISOR

**DR. RUMI DHAR
ASSISTANT PROFESSOR
DEPARTMENT OF LAW
NAGALAND UNIVERSITY, LUMAMI**

SUBMITTED

**IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE
DEGREE OF DOCTOR OF PHILOSOPHY IN LAW OF NAGALAND
UNIVERSITY**



नागालैण्ड विश्वविद्यालय NAGALAND UNIVERSITY

(संसद द्वारा पारित अधिनियम 1989, क्रमांक 35 के अंतर्गत स्थापित केंद्रीय विश्वविद्यालय)
(A Central University established by an Act of Parliament No.35 of 1989)
मुख्यालय : लुमामी, जिला : जुन्हेबोटो (नागालैण्ड), पिनकोड – 798627
Hqrs : Lumami, Dist. Zunheboto (Nagaland), Pin Code – 798627
वेबसाइट / Website : www.nagalanduniversity.ac.in

Ref No.

Date:

CERTIFICATE

This is to certify that the thesis entitled “*A Critical Legal Study on Data Protection Laws in India and Its Applicability in The State of Nagaland*” which is submitted herewith for the Degree of Philosophy in Law of Nagaland University is the result of the original work completed by *Miss Sonia Nath (Regd. No. Ph.D./LAW/00705)* under my supervision and guidance. To the best of my knowledge, the work embodied in this thesis has not been studied previously in the context of any previous degree awarded by any other university or institute. This thesis is fit for submission and evaluation.

This thesis may therefore be placed before the External Examiner for evaluation.

Dr. Kuldeep Singh Panwar
(Head)

Dr. Rumi Dhar
(Supervisor)

NAGALAND UNIVERSITY
APRIL 2026

DECLARATION

I, **Ms. Sonia Nath**, hereby declare that the subject matter of this Thesis is the record of work done by me, that the contents of this Thesis did not form the basis of the award of any previous degree to me or to the best of my knowledge to anybody else, and that the thesis has not been submitted by me for any research degree in any other University/Institute. This is being submitted to the Nagaland University for the degree of Doctor of Philosophy in Law in the Department of Law.

Ms. Sonia Nath

(Scholar)

Reg No: Ph.D/LAW/00705

Date:

Dr. Rumi Dhar

(Supervisor)

Assistant Professor

Department of Law

Nagaland University, Lumami

Date:

Dr. Kuldeep Singh Panwar

(Head)

Associate Professor

Department of Law

Nagaland University, Lumami

Date:

NAGALAND UNIVERSITY
Plagiarism Self Declaration Certificate

Name of Scholar	Ms. Sonia Nath	
Registration Number	PhD/LAW/00705 dated 13-09-2022	
Title of PhD Thesis	A Critical Legal Study on Data Protection Laws in India and Its Applicability in The State of Nagaland	
Name & Institutional Address of the Supervisor	Dr. Rumi Dhar Department of Law, Nagaland University, Lumami, Nagaland- 798627, Zunheboto, India.	
Name of the Department and School	Department of Law, School of Social Science.	
Date of submission	23-04-2026	
Date of plagiarism check	23-04-206	
Name of the software used	DrillBit	
Percentage of similarity detected by the software	Core Areas	10%
	Non-Core areas	

I hereby declare that the Ph.D. Thesis submitted by me is complete in all respects, as per the guidelines of the UGC/NU for this purpose. I also certify that the Thesis (soft copy and print version) has been checked for plagiarism using DrillBit similarity check software. A copy of the Report generated by the software is also enclosed.

Place: Lumami
Date:

(Name & Signature of the Scholar)

Dr. Rumi Dhar

Name & Signature of the Supervisor with seal:

Dr. Kuldeep Singh Panwar

Name & Signature of the Head with seal:



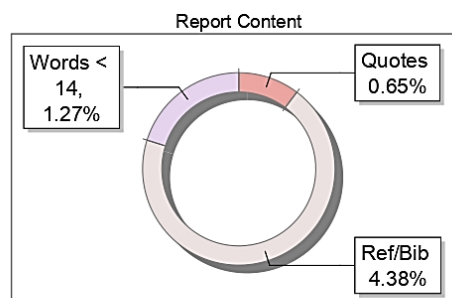
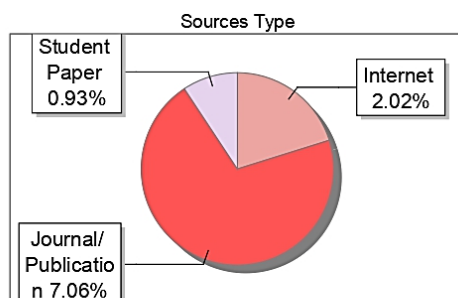
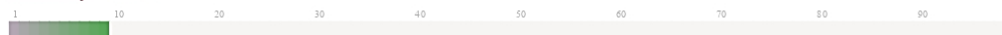
The Report is Generated by DrillBit Plagiarism Detection Software

Submission Information

Author Name	Sonia Nath
Title	A CRITICAL LEGAL STUDY ON DATA PROTECTION LAWS IN INDIA AND ITS APPLICABILITY IN THE STATE OF NAGALAND
Paper/Submission ID	5529099
Submitted by	rumidhar@nagalanduniversity.ac.in
Submission Date	2026-04-23 09:57:54
Total Pages, Total Words	309, 94315
Document type	Thesis

Result Information

Similarity **10 %**



Exclude Information

Quotes	Excluded
References/Bibliography	Excluded
Source: Excluded < 14 Words	Excluded
Excluded Source	7 %
Excluded Phrases	Not Excluded

Database Selection

Language	English
Student Papers	Yes
Journals & publishers	Yes
Internet or Web	Yes
Institution Repository	Yes

A Unique QR Code use to View/Download/Share Pdf File



ACKNOWLEDGEMENT

The successful completion of this doctoral research marks not only the culmination of an academic pursuit but also a journey of personal growth and perseverance. It would not have been possible without the guidance, encouragement, and support of my supervisor, parents, family members, friends and institutions who contributed to my progress in various ways. This acknowledgement is a humble expression of my gratitude to all those whose inspiration, assistance, and goodwill have been instrumental in shaping my research and in making this scholarly endeavour a meaningful and fulfilling experience.

First and foremost, I express my deepest gratitude to my supervisor, Dr Rumi Dhar, for her invaluable guidance, continuous encouragement, and unwavering support throughout my doctoral journey. Her profound insights and constructive feedback have been instrumental in shaping the direction and quality of my research.

I extend my heartfelt thanks to the Head of Department, Dr Kuldeep Singh Panwar, and all my teachers of the Department of Law, Nagaland University, whose knowledge, mentorship, and encouragement have greatly contributed to my academic and personal development over the years. I am grateful to Nagaland University for providing me with the opportunity, resources, and conducive research environment necessary to pursue my doctoral studies.

I am deeply indebted to my family for their unconditional love, patience, and belief in me. Their constant support has been the foundation upon which I have built every step of this journey. To my parents, who taught me the value of perseverance and curiosity, and to my siblings and best friends, for being my anchor through every challenge. Finally, to all those who, in one way or another, contributed to this journey of learning, I am sincerely grateful.

LIST OF ABBREVIATIONS

A	
ABDM	Ayushman Bharat Digital Mission
ACR	Annual Confidential Report
ADM	Automated Decision-Making
AI	Artificial Intelligence
AIA	Algorithmic Impact Assessment
AIDA	Artificial Intelligence and Data Act
APEC	Asia-Pacific Economic Cooperation
APIs	Application Programming Interface
APPI	Act on the Protection of Personal Information 2003
B	
BCRs	Binding Corporate Rules
BPO	Business Process Outsourcing
BSN	Blockchain Service Network
C	
CAC	Cyberspace Administration of China
CBPR	Cross-Border Privacy Rules
CCPA	California Consumer Privacy Act 2018
CERT-In	Computer Emergency Response Team
CICRA	Credit Information Companies (Regulation) Act, 2005
CISO	Chief Information Security Officer
CJEU	Court of Justice of the European Union
COPA	Children's Online Privacy Protection Act 1998
CPPA	Consumer Protection Act
CPRA	California Privacy Rights Act 2020
CRMs	Customer Relationship Management
CSCRF	Cybersecurity and Cyber Resilience Frameworks
D	
DBT	Direct Benefit Transfer
DC	District Commissioner
DCUs	Digital Credit Users
DCPs	Digital Credit Providers
DF	Data Fiduciaries
DGPSI	Data Governance and Protection Standard of India
DIO	District Informatics Officer
DPA	Data Protection Authority

DPBI	Data Protection Board of India
DPDP Act	Digital Personal Data Protection Act 2023
DPDP Rules	Digital Personal Data Protection Rules 2025
DP Law	Data Protection Law
DPO	Data Protection Officer
DPIAs	Data Protection Impact Assessments
DSA	Data Structures and Algorithms
E	
ECHR	European Court of Human Rights
EDPB	European Data Protection Board
EPRS	European Parliamentary Research Service
EU	European Union
F	
FDE	Full-disk Encryption
FE	File-based Encryption
FIG	Figure
FISA	Foreign Intelligence Surveillance Act 1978
FRB	Foreign Re-Insurance Branches
G	
GCI	Global Cybersecurity Index
GDPR	General Data Protection Regulations
GE	General Electric
GIS	Geographic Information System
H	
HIPAA	Health Insurance Portability and Accountability Act 1996
HRESIA	Human Rights and Ethical Impact Assessment
I	
IBEF	India Brand Equity Foundation
ICMR	Indian Council of Medical Research
ICT	Information and Communication Technology
ICRIER	Indian Council for Research on International Economic Relations
IDP	India Dataset Platform
IoT	Internet of Things
IPCIDE	ICRIER Prosus Centre for Internet and Digital Economy.
IRDAI	Insurance Regulatory and Development Authority of India
IS	Information Security
ITES	Information Technology Enabled Services
IT Rule	Information Technology Rules

ITU	International Telecommunication Union
J	
JSON	JavaScript Object Notation
K	
KYC	Know Your Customer
L	
LDCs	Least Developed Countries
LGPD	Lei Geral de Proteção de Dados (General Data Protection Law) Brazil
LSPs	Lending Services Providers
M	
MeitY	Ministry of Electronics and Information Technology
MGNREGA	Mahatma Gandhi National Rural Employment Guarantee Act
MIIT	Ministry of Industry and Information Technology
ML	Machine Learning
MTPA	Medical Termination of Pregnancy (MTP) Act 1971
N	
NBFC	Non-Banking Financial Company
NCR	National Capital Region
NDHE	National Digital Health Ecosystem
NDHM	National Digital Health Mission
NEFA	North-East Frontier Agency
NHA	National Health Authority
NHTA	Naga Hills and Tuensang Area
NIC	National Informatics Centre
NITI Aayog	National Institution for Transforming India
NPC	Naga People's Convention
NPD	Non-Personal Data
NoSQL	Not Only SQL
NSWAN	Nagaland State Wide Area Network
O	
OECD	Organization for Economic Co-operation and Development
OHCHR	Office of the High Commissioner for Human Rights
OLAP	Online Analytical Processing
ONDC	Open Network for Digital Commerce
OPC	Office of the Privacy Commissioner of Canada
P	
PDPA	Personal Data Protection Act 2012
PIA	Privacy Impact Assessment

PIL	Public Interest Litigation
PIPC	Personal Information Protection Commission
PIPEDA	Personal Information Protection and Electronic Documents Act 2000
PIPA	Personal Information Protection Act 2011
PIPL	Personal Information Protection Law 2021
POPIA	Protection of Personal Information Act, 2013
R	
RBI	Reserve Bank of India
REs	Regulated Entities
RRBs	Regional Rural Banks
RTI	Right to Information
S	
SAMR	State Administration for Market Regulation
SBI	State Bank of India
SCCs	Standard Contractual Clauses
SDF	Significant Data Fiduciaries
SDI	Spatial Data Infrastructure
SIDS	Small Island Developing States
SEBI	Securities and Exchange Board of India
SPD	Sensitive Personal Data
T	
TRAI	Telecom Regulatory Authority of India
U	
UDHR	Universal Declaration of Human Rights
UIDAI	Unique Identification Authority of India
UK	United Kingdom
UPI	Unified Payments Interface
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Educational, Scientific and Cultural Organization
US	United States
X	
XML files	Extensible Markup Language Files

LIST OF TABLES

Table No	Title	Page No
1.1	Distribution of respondents	36
2.1	Key differences between various drafted Data Protection Bills	68
5.1	Comparative Analysis of DPDPD Act with Global Data Protection Laws	213
6.1	Respondents age distribution	221
6.2	Gender distribution of respondents	222
6.3	Residence of the respondents	223
6.4	Familiarity across Age Groups	225
6.5	Awareness about rights	227
6.6	Data Breach Experiences	229
6.8	Organizational transparency practice	239
6.9	DPDPA Adequately Addresses Data Protection Issues	242
6.10	Adequacy Opinion Across Age Groups	242
6.11	Relationship Between Age and Awareness (Chi-square test results)	243
6.12	Opinion on Data protection laws need to be modified	244
6.13	Chi-Square Test Results	244
6.14	Should Nagaland create its own data protection policies	245
6.15	Descriptive Analysis (Mean Rank)	246
6.16	Kruskal-Wallis Test Results	246
6.17	Citizens' Perceptions on Digital Infrastructure	247
6.18	Chi-Square Test Result of Digital Infrastructure across age groups	248
6.19	Public Opinion on Digital Literacy	249
6.20	Chi-Square Test Result (Digital Literacy and Implementation)	249
6.21	Descriptive Analysis for Nagaland Digital Infrastructure	250
6.22	Crosstab (Age group and Support for Digital Infrastructure)	251

6.23	Chi-Square Independent Test Result	251
6.24	Data Protected over Online Service	252
6.25	Opinion on Data over Online Services across age groups	253
6.26	Chi-Square Test Result (Online Data Safety)	253
6.27	People's Perception of Data Localization	254
6.28	People's Perception of Data Localization Across Age Groups	255
6.29	Chi-Square Test Result (Perception of Data Localization)	255
6.30	Perception about Cross-Border Data Transfer	256
6.31	Perception about Cross-Border Data Transfer across Age Groups	257
6.32	Chi-Square Test Result (Perception of Cross-Border Data Transfer)	257

LIST OF FIGURES

Sl no	Name of Figures	Page no
1.1	Data Protection and Privacy Legislation Worldwide	8
2.1	Timeline of Indian Data Protection Laws	69
6.1	Educational Qualifications of the Respondents	222
6.2	Occupational Status of Respondents	223
6.3	Familiarity with the term Data Protection	224
6.4	Awareness about the DPDP Act	225
6.5	Read about Data Protection	226
6.6	Public Awareness Campaign	226
6.7	Awareness about Rights	228
6.8	Data Breach Experiences	229
6.9	Perception of technologies	230
6.10	Public opinion on the regulation of emerging technologies	231
6.11	Frequency of Password Change	232
6.12	Frequency of Website policy checking	232
6.13	Data Privacy at Workplace	238
6.14	Which sector require more attention	238

CONTENTS

	<i>Page No</i>
<i>Certificate</i>	I
<i>Declaration</i>	II
<i>Plagiarism Free Undertaking</i>	III
<i>Plagiarism Report</i>	IV
<i>Acknowledgement</i>	V
<i>Abbreviations</i>	VI-IX
<i>List of Tables</i>	X-XI
<i>List of Figures</i>	XII

CHAPTER 1: INTRODUCTION

1.1	Introduction	1-5
1.2	Background of the Study	6-9
1.3	Definition of Key Terms	9-13
1.4	Nagaland and Digital Personal Data Protection Act 2023	13-16
1.5	Review of Literature	
	1.5.1 Books	16-21
	1.5.2 Article	22-28
	1.5.3 Research Gap	28-29
1.6	Statement of the Problem	29-30
1.7	Research Objectives	30-31
1.8	Significance of the Study	31
1.9	Research Questions	32
1.10	Hypotheses	32
1.11	Research Methodology	
	1.11.1 Data Collection	33-35
	1.11.2 Sampling Design	35-36
	1.11.3 Tabulation and Presentation	36-37
1.12	Limitations of the Study	38
1.13	Scheme of Chapterization	38-40

CHAPTER 2: GENESIS OF DATA PROTECTION LAWS IN INDIA

2.1	Introduction	41-42
2.2	Emergence of Data Protection Laws in India	
2.2.1	Early Beginning: Pre-Independent India	43-45
	(a) The Indian Telegraph Act 1885	
2.2.2	Post-Independence Era (1947- 2000)	45-48
	(a) Late 1980s Legal Development	
2.3	Initial Legal Frameworks in India from 2000 to 2011	48-50
2.3.1	Information Technology Act 2000	50-51
2.3.2	The Credit Information Companies (Regulation) Act 2005	51-52
2.3.3	Information Technology (Amendment) Act 2008	53-54
2.3.4	Information Technology (SPD) Rules, 2011	54-55
2.3.5	Information Technology (Intermediaries Guidelines) Rules, 2011 and Information Technology Rule 2021	55-56
2.3.6	Aadhar and the Rise of Digital Identity	57-58
2.3.7	The Judicial Push: Recognition of Privacy as a Fundamental Right	58-61
2.4	Reports of Various Committees	
2.4.1	The Justice A.P. Shah Committee (2012)	61-62
2.4.2	Justice B.N. Srikrishna Committee (2018)	62-63
2.5	Data Protection Bills	
2.5.1	Personal Data Protection Bill, 2019	63-64
2.5.2	Data Protection Bill 2021	64-65
2.5.3	Digital Personal Data Protection Bill, 2022	65-66
2.5.4	Digital Personal Data Protection Bill 2023	66-67
2.5.5	Comparative Analysis Data Protection Bills: A Snapshot	67-68
2.6	Digital Personal Data Protection Act, 2023	
2.6.1	Key Concepts and Definitions under the Act	70-72
2.6.2	The Key Features of the Act.	72-73
2.6.3	Principles of Data Privacy	73-74
2.6.4	Rights and Obligations under the Act	75-78
2.6.5	Data Protection Board of India	78-79
2.7	Digital Personal Data Protection Rule 2025	79-81

2.8	Nagaland State Data Sharing and Accessibility Policy 2024	81-84
2.9	Conclusion	85-86

CHAPTER 3: CONCEPTUAL FOUNDATION AND MULTILAYERED LEGAL FRAMEWORKS FOR DATA PROTECTION IN INDIA

PART I- DATA AND DATA PRIVACY: CONCEPTUAL FRAMEWORK

3.1	Introduction	87-88
3.2	Understanding Data: Nature, Typologies and Characteristics	
3.2.1	Structured data, Unstructured data and Semi-structured data	88-89
3.2.2	Personal, Non-Personal and Sensitive Personal Data	90-93
3.2.3	Metadata, Big Data, and Inferred Data	93-94
3.2.4	Characteristics of Digital Data (5V)	94-96
3.3	Data Protection and Data Privacy: Legal Conceptual Distinction	97-98
3.4	Risks and Threats to Privacy Rights	
3.4.1	State Surveillance	98-99
3.4.2	E-commerce and Social Media	99-100
3.4.3	Data breach and cyber attacks	100-101
3.4.4	Predictive Profiling and Behavioural Manipulation	101-102
3.5	Tools and Technologies for Data Protection	
3.5.1	Anonymization and Pseudonymization of Data	102-103
3.5.2	Encryption and Homomorphic Encryption of Data	103
3.5.3	Blockchain technology and smart contracts	103-104
3.5.4	Algorithmic Impact Assessment (AIA)	104
3.6	Data Protection Regime: New Wave of Rights	
3.6.1	Right to be forgotten	105-106
3.6.2	Right to Portability	106
3.6.3	Right to Objection to Automated Decision-Making	106-107
3.6.4	Right to Redressal and Algorithmic Fairness	107
3.7	Relevance of Data Protection in the Indian Context	
3.7.1	Rise of the Digital Economy	107-109
3.7.2	Privacy Concerns and Citizens' Autonomy	110-111
3.7.3	Human Rights Implications	111-112

PART II- MULTILAYERED LEGAL REGULATORY FRAMEWORKS

3.8	Constitutional Provisions	112
3.8.1	Article 21 of the Constitution of India	113
3.8.2	Constitutional conflict: Right to Information v Right to Privacy	114-115
3.9	Sector-Specific Regulations- Health Sector	
3.9.1	Draft Health Data Management Policy 2022	115
3.9.2	Medical Termination of Pregnancy Act 2021	116
3.9.3	Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act 1994	116-117
3.9.4	Mental Health Act 2017	117
3.10	Sector-Specific Regulations- Banking and Financial	
3.10.1	Reserve Bank of India	117-120
3.10.2	State Bank of India	120-122
3.10.3	Security and Exchange Board of India	123
3.11	Sector-Specific Regulations- Telecommunication	
3.11.1	Telecommunication Act 2023	124
3.11.2	Telecom Commercial Communication Customer Preference (Second Amendment) Regulations, 2025	125
3.12	Code of Practices and Ethical Guidelines	
3.12.1	ICMR Regulation 2017	125
3.12.2	Online Gaming Norms	126
3.12.3	IRDAI Guidelines	126

PART III- INSTITUTIONAL ARCHITECTURE FOR DATA GOVERNANCE

3.13	Key Institutions for Data Governance	
3.13.1	Ministry of Electronics and Information Technology	127
3.13.2	Indian Computer Emergency Response Team	127
3.13.3	National Informatics Centre (NIC)	127
3.14	Gaps and Challenges in Indian Legal Frameworks	127-128
3.15	Emerging Areas of Concern	129
3.16	Conclusion	129-130

CHAPTER 4: INTERNATIONAL LEGAL FRAMEWORKS ON DATA PRIVACY AND DATA PROTECTION

4.1	Introduction	131-134
4.2	Evolution of International Data Protection Norms	134
4.2.1	Early Developments	135
4.2.2	The Role Of Human Rights Instruments	136
4.2.3	From Soft Law to Binding Instruments	136
4.2.4	Digitalization and the Role of Transitional Data Flows	137-138
4.3	Key International Legal Instruments and Frameworks	
4.3.1	Convention 108+	139-141
4.3.2	APEC Privacy Frameworks	141-143
4.3.3	OECD Guidelines	143-145
4.3.4	UN Initiatives	145-147
4.4	Regional Approach To Data Protection	
4.4.1	European Union: General Data Protection Regulation 2018	148-158
4.4.2	North America- California: Privacy Rights Act 2020	158-164
4.4.3	South America- Canada: Personal Information Protection and Electronic Documents Act 2000	165-172
4.4.4	Africa- South Africa: Protection of Personal Information Act 2013	172-178
4.4.5	Asia- South Korea: Personal Information Protection Act 2011	179-186
4.4.6	Neighbouring Country: China- Personal Information Protection Law 2021	186-193
4.5	Emerging Challenges In International Data Protection	193
4.5.1	Artificial Intelligence And Automated Decision-Making	194
4.5.2	Profiling, Surveillance And Emotional Data	194
4.5.3	Global Cyber Security Alliances And Privacy Dilution	194
4.6	Conclusion	195

CHAPTER 5: CRITICAL APPRAISAL OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

5.1	Introduction	196-197
5.2	Constitutional recognition of the right to privacy	197
5.3	Gaps in Provisions of The DPDP Act 2023	
5.3.1	Vague and Underdefined Core Concepts	198
5.3.2	Absence of Data Classification Tiers	198-199
5.3.3	Unchecked State Power and Blanket Exemptions	199
5.4	Institutional Ecosystem And Enforcement Gaps	
5.4.1	Weak Institutional Design of the Data Protection Board	200
5.4.2	Absence Of Inter-Regulatory Coordination	200-201
5.4.3	Inadequate Grievance Redressal Framework	201
5.5	Cross-Border Data Transfer Mechanisms	201-202
5.6	Surveillance, Intelligence and State Exemptions	202-203
5.7	Algorithmic Governance and Automated Decision-Making	
5.7.1	Lack of Legal Safeguards For AI Profiling	203
5.7.2	Unrecognized Digital Rights in Automated Decision-making Context	204
5.7.3	Emotional And Behavioural Data Exploitation	204
5.7.4	No Risk-Based Regulatory Framework For Algorithms	204
5.8	Data Fiduciary Duties and Accountability Mechanisms	
5.8.1	Limited Scope of Data Fiduciary Obligations	205
5.8.2	Lack Of Procedural Fairness In Processing	205
5.8.3	No Sector-Specific Accountability Provisions	206
5.9	Rights of Data Principal	
5.9.1	Incomplete Recognition of Individual Rights	206
5.9.2	Right to Data Portability and Right to Objection	206
5.9.3	Lack of Collective and Community Data Rights	207
5.10	Regulating Emerging Technologies: AI, IOT, Blockchain	
5.10.1	Regulatory Silence for IOT and Device-Generated Data	207
5.10.2	Incompatibility with Blockchain Technology	207
5.10.3	No Regulation for High-Risk AI Systems	207
5.11	Data Localization and Data Breach Notification	208
5.12	Comparative Study of the Digital Personal Data Protection Act 2023 With Global Legislation	209-213

5.12.1	EU General Data Protection Regulation (GDPR)	209
5.12.2	California Consumer Privacy Act (CCPA)	210
5.12.3	Canada's Consumer Privacy Protection Act (CPPA)	210-211
5.12.4	South Korea's PIPA	211
5.12.5	China's Personal Information Protection Law (PIPL)	212
5.13	Limitations of Digital Personal Data Protection Rule 2025	214-217
5.14	Bridging The Gaps: Pathways for Policy Reforms	
5.14.1	Institutional Innovation And Structural Reform	217
5.14.2	Risk-Based And Rights-Based Processing System	218
5.14.3	Enforcement Ecosystem	218
5.14.4	Cross-Border Data Transfer	218
5.14.5	Algorithmic transparency and automated decision-making	219
5.14	Conclusion	219

CHAPTER 6: ASSESSING THE APPLICABILITY OF DATA PROTECTION LAWS IN THE STATE OF NAGALAND: AN ANALYSIS

6.1	Introduction	220
6.2	Demographic Profile of Respondents	221-223
6.3	People's perceptions on Data privacy and rights	224-233
6.4	Hypotheses Testing	233-259
6.5	Answer to Research Question	259-267
6.6	Applicability of Data Protection Laws in Nagaland	267-272
6.7	Challenges in Effective Implementation of Data Protection Laws	272-275
6.8	Conclusion	275

CHAPTER 7: FINDINGS, CONCLUSIONS, AND SUGGESTIONS

7.1	Introduction	276-277
7.2	Summary of Chapter	277-279
7.3	Key Findings of the Study	279-283
7.4	Conclusion	283-284
7.5	Suggestions and Recommendations	284-286
7.6	Contribution to the Society	287

BIBLIOGRAPHY	288-305

ANNEXURES

Annexure – I	Questionnaire and Interview Schedule
Annexure – II	Survey Consent Form
Annexure – III	Digital Personal Data Protection Act 2023.
Annexure – IV	Digital Personal Data Protection Rules 2025.
Annexure – V	Nagaland State Data Sharing and Accessibility Policy 2024.
Annexure – VI	IEC Certificate
Annexure – VII	List of Publications
Annexure – VIII	List of Paper Presentations
Annexure – IX	List of Workshops attended
Annexure – X	Patent Design Certificate

CHAPTER -1

INTRODUCTION

1.1 INTRODUCTION

In an increasingly digitalized world, the boundaries of law, technology, and governance are rapidly shifting. The 21st century has witnessed an unprecedented explosion in the collection, processing, and monetization of personal data, ushering in what is now referred to as the ‘*datafied societies*’¹. From biometric authentication under Aadhaar to predictive algorithms on social media, individual identities are no longer confined to physical or social realities; they are increasingly abstracted into digital profiles, vulnerable to surveillance, commodification, and algorithmic discrimination. Globally, data has been termed the *new oil*², but unlike natural resources, its extraction often occurs without the knowledge or meaningful consent of the data subject. In India, the scale of data generation is staggering. As of 2024, India had over 1.2 billion digital identities under the Aadhaar system³, with over 850 million active internet users. In January 2025, UPI transactions surpassed 16.99 billion, with a value exceeding 23.48 lakh crore. As per the report of Brickwork, the Indian e-commerce market is expected to grow at a compound annual growth rate of 27% to reach \$ 163 billion by 2026⁴. According to the India Brand Equity Foundation (IBEF) website, India’s Business-to-Business (B2B) online marketplace is projected to be a US\$200 billion opportunity by 2030⁵. The proliferation of digital public infrastructure, including DigiLocker, UPI, and CoWIN, has further embedded data into everyday governance. However, this rapid digital transformation has created a

¹ Arne Hintz, Lina Dencik, et al., *Civic Participation in the Datafied Society: Towards Democratic Auditing?*, Data Justice Lab, 2022, https://datajusticelab.org/wp-content/uploads/2022/08/CivicParticipation_DataJusticeLab_Report2022.pdf.

² Marcin Szczepanski, *Is Data The New Oil? Competition Issues In The Digital Economy*, European Parliamentary Research Service (EPRS), Jan 2020, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI\(2020\)646117_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf).

³ Ministry of Electronics and Information Technology (MeitY) Government of India, *Annual Report 2021-2022*, <https://www.meity.gov.in/static/uploads/2024/02/31-1.pdf>, (Last visited Dec. 05, 2024).

⁴ Brickwork Rating, *E-Commerce Market in India*, Brickwork Research, October 2024, <https://www.brickworkratings.com/Research/E-RetailIndustryinIndia-Oct2024.pdf>.

⁵ India Brand Equity Foundation (IBEF), <https://www.ibef.org/industry/ecommerce>, (Last visited Dec. 12, 2024).

regulatory vacuum, exposing serious concerns about data privacy, security, autonomy, and accountability. The absence of a dedicated data protection regime for decades has had tangible consequences. Several high-profile data breaches across the public and private sectors have highlighted the vulnerability of Indian data infrastructure and the inadequacy of legal safeguards. In 2018, a journalistic investigation revealed that access to Aadhaar data could be purchased for as little as ₹ 500, raising doubts about the integrity of the Unique Identification Authority of India (UIDAI) and its security architecture⁶. However, the same has been denied by the UIDAI through a Press Note on 4th January 2018 at 4:15 P.M⁷. In 2021, a cyberattack on Air India compromised the personal data, including passport and credit card details, of over 4.5 million passengers⁸. The Domino's India data breach exposed geolocation data and consumer profiles of over 18 crore orders⁹, and more recently, the CoWIN data exposure through a Telegram bot (2023) demonstrated that merely inputting a phone number could reveal a citizen's Aadhaar-linked vaccination data, including gender, age, and identification numbers¹⁰. This incident reflects not an isolated technical failure but a systemic weakness in India's data governance framework, particularly its inability to guarantee informational privacy and ensure legal recourse.

Before the enactment of the Digital Personal Data Protection Act 2023, India did not possess a standalone, comprehensive legislation specifically dedicated to the protection of personal data. Instead, the legal framework governing data privacy operated in a fragmented and largely sector-specific manner. The primary statutory

⁶ Rachna Khaira, Rs 500, 10 minutes, and you have access to billion Aadhaar details, The Tribune, <https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361/>, (Updated Jan 04, 2018, At : 07:37 AM IST).

⁷ Press Note, Ministry of Electronics and IT, January 04, 2018, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1515503#:~:text=Unique%20Identification%20Authority%20of%20India,no%20access%20to%20biometric%20details>, (Last visited Dec. 10, 24).

⁸ Poulomi Saha, *Air India Data Breach: Personal Info of 45 Lakh People Leaked Due To Sophisticated Cyberattacks*, India Today, <https://www.indiatoday.in/india/story/air-india-data-breach-personal-info-of-45-lakh-people-leaked-sophisticated-cyberattack-1805528-2021-05-21>, (Updated May 22, 2021, 14:22 IST).

⁹ Srivatsan KC, *Domino's Pizza Data Breach: Company Says Financial Information Safe As Data of 180 Million Users Compromised*, Hindustan Times, <https://www.hindustantimes.com/india-news/dominos-pizza-data-breach-company-says-financial-information-safe-as-data-of-180-million-users-compromised-101621855567340.html>, (Updated May 24, 2021, 05:30 PM IST).

¹⁰ John Xavier, *Explained What does the alleged CoWIN data leak reveal?*, The Hindu, <https://www.thehindu.com/sci-tech/technology/explained-what-does-the-alleged-cowin-data-leak-reveal/article66980831.ece>, (Updated June 18, 2023, 01:23 PM IST).

protection for personal data was provided under Section 43A¹¹ and 72A¹² of the Information Technology Act, 2000¹³ (as amended in 2008), which impose civil liability and criminal penalties on companies for negligent handling or unauthorized disclosure of sensitive personal data. Supplementing these provisions, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rule 2011¹⁴ offered a definition of sensitive data and prescribed compliance requirements for corporate entities. However, these rules applied exclusively to private bodies, excluding government departments, and thereby creating a critical gap in public sector data accountability. In 2021, the Government of India further expanded the regulatory landscape through the promulgation of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rule 2021¹⁵. These rules significantly altered the obligations of intermediaries, social media platforms, and digital news publishers, mandating stricter compliance with content moderation, user traceability, and grievance redressal protocols. Although the IT Rule 2021 is not a data protection law in a strict sense.

The absence of statutory precision meant that enforcement mechanisms were weak, judicial remedies limited, and compliance by both public and private actors was highly discretionary. Sectoral regulation, such as that issued by the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India (IRDAI) and the Telecom Regulatory Authority of India (TRAI), added further layers, but often without coherence or uniformity. In the cases of *Karmanya Singh Saren v Union of India* (2017),¹⁶ *Pallav Mangia v Union of India* (2017)¹⁷ and *M/S Intex Technology (India) Ltd v Ashok Kumar* (2016),¹⁸ concerns about the data privacy breach in the digital world have raised concerns about the inadequacy of existing laws. In response

¹¹ The Information Technology Act, 2000, § 43A- Compensation for failure to protect data (India).

¹² The Information Technology Act, 2000, § 72A- Punishment for disclosure of information in breach of lawful contract, (India).

¹³ The Information Technology Act, 2000, No. 21, Act of Parliament, 2000, (India).

¹⁴ The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rule 2011, GSR 313 (E), (India).

¹⁵ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rule 2021, GSR 139 E, (India).

¹⁶ *Karmanya Singh Saren v Union of India*, SLP (Special Leave Petition (Civil) No. 804 of 2017).

¹⁷ *Mangia v Union of India*, WP (C) No 347 of 2017.

¹⁸ *M/S Intex Technology (India) Ltd v Ashok Kumar* CS (OS) 487/ 2016.

to mounting public pressure and judicial mandates, the Supreme Court in the landmark judgment of *Justice K S Puttaswamy v Union of India* (2017) ¹⁹ recognized the right to privacy as a fundamental right. This judgment did not immediately trigger the enactment of a robust data protection regime. In the case of *Naveen Kumar R @ Naveen v State of Karnataka* (2023),²⁰ the court has expressed concern for the increasing incidents of data theft in the digital age. It took six years, and multiple draft bills from the Shrikrishna Committee Report to the Personal Data Protection Bill 2019, before the *Digital Personal Data Protection Act (DPDP Act) 2023*²¹ was finally enacted. The DPDP Act 2023 is a landmark in Indian digital law, establishing for the first time a statutory framework for data principals (users/ data owners) and data fiduciaries (entities processing data).

The Act aims to create a comprehensive legal framework for the protection of personal data in India. It defines foundational categories, such as *data principal*, *data fiduciary*, and *consent manager*, and incorporates principles, including *purpose limitation*, *data minimization*, and *lawful processing* based on informed consent. It grants the data principal certain enforceable rights, including the right to access, correction, erasure, nomination, and grievance redressal. It introduces a Data Protection Board of India as the regulatory authority to oversee compliance and adjudicate disputes. Despite its legislative enactment in August 2023, the Digital Personal Data Protection Act has not come into force as of 2025. The Ministry of Electronics and Information Technology, through its notification dated November 13, 2025, notifies that significant provisions of the Act will become operational between late 2026 and mid-2027. The notification specifies that different provisions of the Act and rules come into force at different times rather than all at once. The G.S.R. 843 (E) provides phase-wise commencement of the Act, such as sections 1(2), 2, 18-26, 35, 38-43 and section 44(1) and 44(3) take effect immediately upon publication of the Official notifications. One year later, section 6(9) and section 27(1)(d) will come into force. Eighteen months after publication, the core rights, obligations, and compliance mechanisms under sections 3-17 and 27-34. 36-37 and 44(2) will become

¹⁹ Justice K S Puttaswamy (Retd) and Anr v Union of India (2017) 10 SCC 1, AIR 2017 SC 4161.

²⁰ Naveen Kumar R @ Naveen v State of Karnataka- Criminal Petition No 3173 of 2023.

²¹ Digital Personal Data Protection Act, 2023, (No 22), Act of Parliament 2023, (India).

operational²². The implementation of the Digital Personal Data Protection Rules 2025 is spread out over multiple dates or phases. For instance, Rules 1, 2, and 17-21 will take effect immediately, while Rule 4 will take effect after one year. Rules 3, 5-16, 22, and 23 will take effect after eighteen months²³. The amendments to the Right to Information Act, 2005, which limit access to personal information even when there is a strong public interest, have already come into force. This immediate change raises notable concerns among transparency activists²⁴. The Digital Personal Data Protection Act 2023 has been criticized by many on the grounds that:

- Clause 17(2): which grants the Central Government sweeping power to exempt any state agency from the provisions of the Act “*in the interest of sovereignty, national security or public order*”.
- No formal mechanism exists for state participation in data governance, even though digital data intersects with health, agriculture, and land records, all are State List subjects.
- The Data Protection Board of India, though nominally independent, is controlled by the executive, raising questions about institutional autonomy.

The study seeks to critically examine the multifaceted dimensions influencing the applicability of data protection laws in the State of Nagaland, within the broader framework of India’s evolving digital governance framework. The study examines the applicability of national data protection laws to the State of Nagaland. It explores whether national data protection laws are legally and practically enforceable within Nagaland’s socio-legal context. It seeks to determine the extent, limitations and effectiveness of applying national data protection laws in Nagaland, and whether state-specific adaptations or harmonized legal frameworks are necessary for effective data governance.

²² Ministry of Electronics and Information Technology Notification, GSR 843 E, The Gazette of India, Pt. II, Sec 3(i), Nov. 13, 2025.

²³ Ministry of Electronics and Information Technology Notification, GSR 846 E, The Gazette of India, Pt. II, Sec 3(i), Nov. 13, 2025.

²⁴ Aroon Deep, “*Digital Personal Data Protection Act Notified After Two Years, RTI Act Amended*,” The Hindu, <https://www.thehindu.com/news/national/digital-personal-data-protection-act-notified-after-two-years-rti-act-amended/article70278698.ece>, (Updated November 14, 2025, 08:58 PM IST).

1.2 BACKGROUND OF THE STUDY

The rise of the digital age has profoundly reshaped not only how societies function but also how individuals relate to the State, corporations, and one another. At the heart of transformation lies data, a resource often described as the new oil, but perhaps more accurately understood as the lifeblood of modern governance, commerce and communication. From biometric authentication systems like Aadhaar to location tracking on smartphones, individuals today leave a continuous trail of digital footprints that are constantly harvested, analyzed, and monetized. As the scale and sophistication of data collection increase, so too does the need to understand what constitutes data, how it is classified, how its protection has evolved, and why safeguarding it is more urgent than ever. The genesis of data protection laws can be traced back to the late 19th century, when American lawyers Samuel Warren and Louis Brandeis published their seminal article “*The Right to Privacy*”²⁵ in the Harvard Law Review, describing privacy as “*the right to be let alone*”²⁶. Historically, legal systems have protected personal space and reputation through torts like defamation and breach of confidentiality²⁷.

The earliest legal articulation of data protection can be traced to Germany, where the State of Hesse enacted the world’s first data protection law in 1970²⁸. Whereas Sweden was the first nation to enact a data privacy law in 1973,²⁹ and following the trend, France,³⁰ Denmark, Austria, and Norway passed data privacy laws in 1978. The turning point in the global data protection movement came with the Organization for Economic Co-operation and Development (OECD) Guidelines on

²⁵ Samuel D Warren, and Louis D Brandeis, *The Right to Privacy*, Vol. 4, No. 5, HARVARD LAW REVIEW, 193-220, (1890), <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>.

²⁶ Ana Mishova, *Data Protection Laws Around the World: A Global Perspective*, GDPR Local, August 16, 2024, <https://gdprlocal.com/da3ta-protection-laws-around-the-world-a-global-perspective/>, (Last visited Dec. 08, 2024).

²⁷ David Mangan, *The Relationship Between Defamation, Breach of Privacy and Other Legal Claims Involving Offensive Internet Content, Defamation Law in the Internet Age*, Commissioned by the Law Commission of Ontario, July 2017, <https://www.lco-cdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-Mangan-1.pdf>, (Last visited Dec. 10, 2024).

²⁸ Data Protection Act 1970, Federal Republic of Germany, dated Oct. 07, 1970.

²⁹ Data Protection Act 1973 (SFS no.: 1973:289), 1973-05-11, https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289/.

³⁰ The French Data Protection Act 1978, Act 78-17 (Jan. 06, 1978) <https://www.ssi.ens.fr/textes/a78-17-text.html>.

the Protection of the Privacy and Transborder Flows of Personal Data (1980). These guidelines outline core principles, including purpose limitation, data minimization, individual participation, and accountability. OECD acknowledge the need to balance privacy with legitimate governmental and commercial interests, setting the stage for global convergence on data norms. In the ensuing decades, Europe emerged as a leader in the field, culminating in the adoption of the European Union's Data Protection Directives in 1995 (Directive 95/46/EC), which laid the foundation for harmonized privacy rights across member states. Meanwhile, other jurisdictions have developed a distinct but comparable framework. The United States has adopted a sectoral approach, regulating specific industries such as healthcare. At the State level, California's Consumer Privacy Act of 2018 and its successor, California Privacy Rights Act of 2020, have moved toward a more unified model. Relevantly, Malaysia became the first country in the Southeast Asia region that enacted its first law aiming to protect personal data, the Personal Data Act in 2010, which came into effect in 2013³¹. To date, a total of 155 of 195 (79%) countries have enacted data protection laws³².

The global landscape of data privacy legislation has seen significant growth in recent years, reflecting a rising awareness of digital rights and personal data protection. As per the data of UNCTAD, Figure 1.1 represents the percentage of Countries with Legislation on Privacy and Data Protection. According to the latest data from the UN Conference on Trade & Development (UNCTAD), 155 out of 195 countries around the world have enacted. In the African region, 40 out of 60 countries implemented data privacy laws; in the Asia-Pacific region, 40 out of 62 countries have implemented them; only 25 of the 44 Least Developed Countries (LDCs) and 19 of 37 Small Island Developing States (SIDS) have active data privacy laws. Developed countries have 51 of 52, and Latin America and the Caribbean, 29 of 33, show high coverage of data privacy laws.

³¹ Md. Toriqul Islam and Md. Ershadul Karim, *The Brief Historical Account of Global Data Privacy Regulations and the Lesson for Malaysia*, *Sejarah: Journal of History Department*, University of Malaysia, 2019, pp 169-186, DOI: 10.22452/sejarah.vol28no2.

³² UNCTAD, Data protection and privacy legislation worldwide, <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>, (Last visited Dec 17, 2023).

Image 1.1 Global map of data privacy law³³

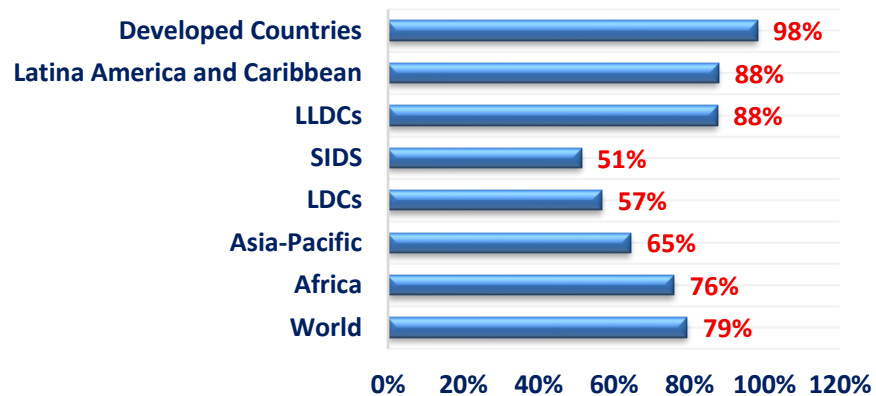
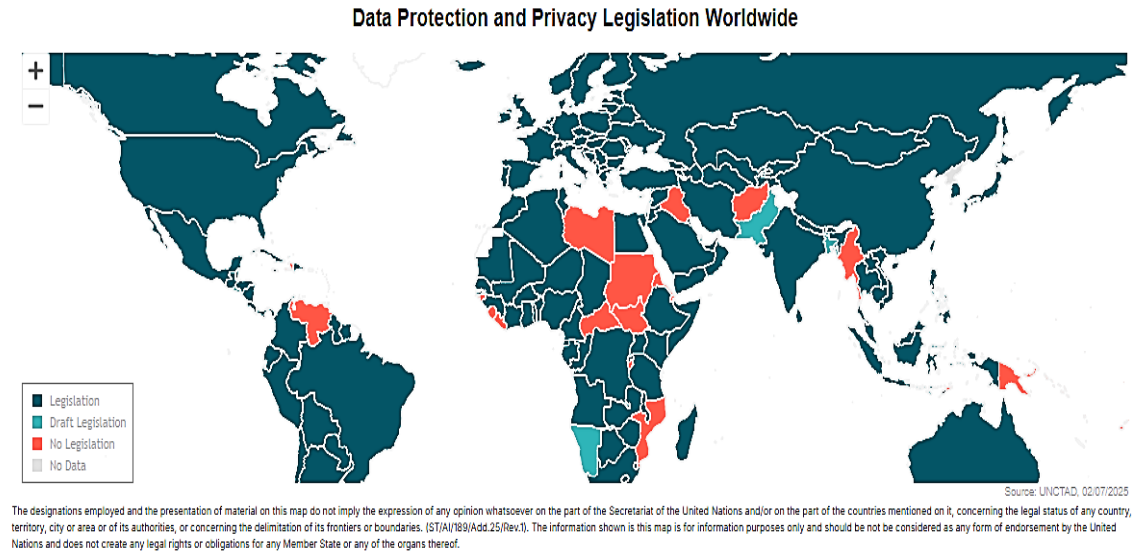


Figure 1.1 Data Protection and Privacy Legislation Worldwide³⁴

India's journey towards data protection has followed the global trend, but with its unique twist and hurdles. For many years, the country relied on the Information Technology Act 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011. But the

³³ UNCTAD, Data protection and privacy legislation worldwide, <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> (Last visited Dec 17, 2023).

³⁴ Id.

judgment of *Justice K S Puttaswamy v Union of India (2017)*³⁵ has sparked a nationwide call for a more comprehensive and dedicated data protection law. In response, the government formed the Srikrishna Committee, which released a pivotal report in 2018. After years of consultations, debates, and multiple draft Bills finally led to the enactment of the Digital Personal Data Protection Act 2023.

1.3 DEFINITION OF KEY TERMS

This section defines the key terms used throughout the thesis, such as data, data principal, data fiduciary, customary law and the Dobashi court.

1.3.1 What is Data?

In the digital age, data encompasses a complex spectrum of meaning that varies across technical, legal, commercial, and cultural contexts. At its most basic level, data refers to any piece of information, whether structured or unstructured, that can be recorded, stored, processed, and communicated. However, as information systems become more sophisticated, the question of what constitutes data and whose data it is has become legally and ethically significant.

Section 2(h) of the Digital Personal Data Protection Act 2023 defines the term Data: *“Data means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means.”*³⁶

IBM defines the term Data as:

*“Data is a collection of facts, numbers, words, observations or other useful information. Through data processing and data analysis, organizations transform raw data points into valuable insights that improve decision-making and drive better business outcomes.”*³⁷

³⁵ Justice K S Puttaswamy v Union of India (2017) 10 SCC 1, AIR 2017 SC 4161.

³⁶ The Digital Personal Data Protection Act (DPDP Act) 2023, § 2(h) (Aug. 11, 2023).

³⁷ Annie Badman and Mathew Kosinski, *What is Data?*, IBM, Oct. 01, 2024, <https://www.ibm.com/think/topics/data>, (Last visited Jan 22, 2025).

The Merriam-Webster Dictionary defines data as,

“(1) Factual information (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation, (2) Information in digital form that can be transmitted or processed, (3) Information output by a sensing device or organ that includes both useful and irrelevant or redundant information and must be processed to be meaningful.”³⁸

i. Personal Data refers to any data that relates to an identifiable individual. Under Section 2(t) of the Digital Personal Data Act 2023, “*personal data means any data about an individual who is identifiable by or in relation to such data*”³⁹. This category is central to most data protection frameworks, and its processing is generally permitted only under strict conditions of informed consent, purpose limitation and data minimization.

ii. Sensitive Personal Data (SPD), though not specifically distinguished in the Digital Personal Data Protection Act 2023, unlike the earlier 2019 draft bill, defines the term

“sensitive personal data as such personal data, which may reveal, be related to, or constitute- financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation”⁴⁰.

Apart from this, Rule 3 of the Information Technology Rule 2011 defines Sensitive Personal Data, or Information means such personal information which consists of information relating to

“password, financial information such as Bank account or credit card or debit card or other payment instrument details, physical, physiological and mental health condition, sexual orientation, medical records and history, biometric information, any details relating to the above clauses as provided to body

³⁸ Data, <https://www.merriam-webster.com/dictionary/data>, (Last visited Dec 17, 2023).

³⁹ The Digital Personal Data Protection Act (DPDP Act) 2023, § 2(t) (India).

⁴⁰ The Personal Data Protection Bill 2019, No. 373, (2019), § 2(36), (India).

corporate for providing services and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise”⁴¹.

iii. Non-Personal Data (NPD) refers to data that does not identify any individual and may consist of aggregated or statistical datasets. Although such data does not typically fall within the scope of privacy laws, its economic and strategic value has led to calls for a separate legal regime. The Committee of Experts on Non-Personal Data Governance (2020) in India has emphasized the need to regulate NPD to ensure data sovereignty. The Committee of Experts defined Non-Personal Data as

“firstly, data that never related to an identified or identifiable natural person, such as data on weather conditions, data from sensors installed on industrial machines, data from public infrastructures, and so on. Secondly, data which were initially personal data, but were later made anonymous. Data which are aggregated and to which certain data transformation techniques are applied, to the extent that individual specific events are no longer identifiable, can be qualified as anonymous data”⁴².

iv. Anonymized Data is personal data that has been processed in such a way that individuals can no longer be identified, either directly or indirectly⁴³.

1.3.2 Data Principal: Section 2(j) of the Digital Personal Data Protection Act 2023 *“Data Principal means the individual to whom the personal data relates, and where such individual is- (i) a child, includes the parents or lawful guardian of such a child;(ii) a person with disability, including her lawful guardian, acting on her behalf”⁴⁴.*

⁴¹ *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011*, Rule 3- Sensitive Personal Data or Information, (India).

⁴² REPORT BY THE COMMITTEE OF EXPERTS ON NON-PERSONAL DATA GOVERNANCE FRAMEWORK, MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOV'T OF INDIA, Dec. 16, 2020, <https://ourgovdotin.wordpress.com/wp-content/uploads/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf>.

⁴³ AEPD, 10 Misunderstanding Related to Anonymisations, (Aug. 08, 2025, 12 PM), https://www.edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf.

⁴⁴ The Digital Personal Data Protection Act (DPDP Act) 2023, § 2(j) (Aug. 11, 2023).

1.3.3 Data Fiduciary: Section 2(i) of the Digital Personal Data Protection Act 2023 defines “*Data Fiduciary as "any person who alone in conjunction with other persons determines the purpose and means of processing of personal data"*”⁴⁵.

1.3.4 Person: Section 2(s) of the Digital Personal Data Protection Act 2023 defines “person” as including- “*an individual, a Hindu Undivided Family (HUF), a company, a firm, an association of persons or a body of individuals, whether incorporated or not, the State and every artificial juristic person, not falling within any of the preceding sub-clauses*”⁴⁶.

1.3.5 Data Protection Laws: For this study, the data protection laws emphasizes the Information Technology Act 2000 and the Amended Act of 2008, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rule 2011, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the Digital Personal Data Protection Act 2023⁴⁷, Draft Digital Personal Data Protection Rules, 2025 and Nagaland State Data Sharing and Accessibility Policy, 2024.

1.3.6 Dobashi Court: In Nagaland, the Dobashi Courts are the customary courts that handle a wide range of civil matters. The Dobashi courts were established for the better administration of justice in Nagaland. The functioning of the Dobashi court is headed by the Head Dobashi of the Customary Court. The decision of this court is subject to a higher Magistrate's court. If the decision given by this court is not satisfactory, the aggrieved party can appeal to the higher court. At present District Dobashi Court is equal in status with that of the second-class Magistrate court⁴⁸. Dobashi were empowered by “Rule for Administration Justice and Police in Naga Hills District 1937”, which has been amended by the State Government of Nagaland

⁴⁵ The Digital Personal Data Protection Act (DPDP Act) 2023, § 2(i) (Aug. 11, 2023).

⁴⁶ The Digital Personal Data Protection Act (DPDP Act) 2023, § 2(s) (Aug. 11, 2023).

⁴⁷ Digital Personal Data Protection Act (DPDP Act) 2023, No 22 Act of Parliament 2023, (India); however, the DPDP Act 2023 is yet to come into force. As per section 1(2) of the DPDP Act, “*it shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint and different dates may be appointed for different provisions of this Act...*”.

⁴⁸ M Imyu Longchar, *Role of Dabashis in Naga Customary Law and Practice*, *Eastern Mirror*, June 9, 2018, <https://www.easternmirrornagaland.com/role-of-dobashis-in-naga-customary-law-practice>, (Last visited Dec. 20, 2024).

from time to time, i.e., the first amendment by 1974⁴⁹, the second amendment in 1983⁵⁰, the third amendment Act 1984⁵¹. The Fourth Amendment Act 1987 was received the assent of the President of India on 4th March 1987, known as “Nagaland Act 1987”. The trial of cases by the Dobashi Court takes a significantly shorter period compared to the Magistrate Court, where numerous legal formalities are involved and result in a longer process with higher costs⁵².

1.4 NAGALAND AND THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

Nagaland was just a district in the State of Assam until 1957, known as “*The Naga Hills*”, the leaders of various Naga Tribes in August 1957, formed the Naga People’s Convention (NPC). Its first session was held in Kohima on August 21, 1957, under the leadership of the late Dr Imkongliba Ao, the Naga People’s Convention (NPC) put forward a significant proposal to create a distinct administrative unit by combining the Tuensang division of the North-East Frontier Agency (NEFA) with the Naga Hills District. The Government of India accepted this proposal on December 1, 1957, and a new administrative region was officially established, named the Naga Hills and Tuensang Area (NHTA)⁵³. A few years later, in July 1960, a delegation from the NPC met with the then Prime Minister of India, Jawaharlal Nehru. Their discussions led to the historic 16-point Agreements, which laid the foundation for the formation of a separate state for the Nagas within the Indian Union. As per the Agreement, this new state, named Nagaland, would be placed under the Ministry of External Affairs and would have key constitutional features, a Governor, an Administrative Secretariat, a Council of Ministers, and a Legislative Assembly. Later, in 1972, administrative oversight of the state was shifted from the Ministry of External Affairs to the Ministry

⁴⁹ The Rules for Administration of Justice and Police in Nagaland (Amendment) Act 1974 (Nagaland Act No 7 of 1974), Gazette Notification Dated Oct. 15, 1974, (India).

⁵⁰ The Rules for Administration of Justice and Police in Nagaland (Second Amendment) Act 1982, (Nagaland Act No 4 of 1983) Gazette Notification Dated Nov. 15, 1983, (India).

⁵¹ The Rules for Administration of Justice and Police in Nagaland (Third Amendment) Act 1984 (Nagaland Act no 1 of 1987) received the assent of the President of India on Mar. 4, 1987, (India).

⁵² *Supra* note 48.

⁵³ History of the NLA, Nagaland Legislative Assembly, Government of Nagaland, <https://webtest.nagaland.gov.in/nla/about-us/>, (Last visited Dec. 01, 2024).

of Home Affairs, where it remains today⁵⁴. The journey toward statehood took a decisive turn on August 21, 1962, when a bill was introduced in the Indian Parliament to grant Nagaland full statehood. The bill was subsequently passed, and on September 4, 1962, it received the assent of the President of India. This legislation came to be known as the State of Nagaland Act 1962, and it officially paved the way for Nagaland to become the 16th State of the Indian Union. The historic transition was completed on December 1, 1963, marking a significant milestone in the political evolution of the Naga people within the framework of the Indian Constitution⁵⁵.

The State of Nagaland was formally inaugurated on December 1, 1963, as the 16th State of the Indian Union. It is bounded by Assam in the west and Myanmar in the east. Arunachal Pradesh and part of Assam to the North, and Manipur to the South. The state consists of 17 Administrative Districts, inhabited by 17 major tribes along with other sub-tribes. Each tribe is distinct from the other in terms of customs, language and dress. Known as the Falcon capital⁵⁶ of the world and home to the spiciest chilly on the planet, this state is a treasure trove of diverse indigenous tribes and dialects, with 17 tribes and over 60 dialects spoken. As per the report of NITI Aayog, March 2025,⁵⁷ Nagaland has a population of 2.2 million, representing 0.2 percent of the country's total population. As per the details from Census 2011, Nagaland has a population of 19.79 lakhs, the total population was 1,990,036, of which males were 1,047,141 and females were 9,42,895 (projected population in 2026 is 47.10 lakhs). Sex Ratio in Nagaland is 931, i.e. for every 1000 males, which is below the national average of 940 as per the latest census⁵⁸. Recognizing the distinct ethnic identity, traditional practices, and historical consciousness of the Naga People, the Constitution of India extended special protections to Nagaland under Article 371(A).

⁵⁴ *Supra* note 53.

⁵⁵ *Supra* note 53.

⁵⁶ Rising Northeast Investors Summit 2025, <https://risingnortheast.in/nagaland/>, (Last visited Nov. 1, 2025).

⁵⁷ *Macro and Fiscal Landscape of the State of Nagaland*, NITI Aayog, Mar 2025, <https://niti.gov.in/sites/default/files/2025-03/Macro-and-Fiscal-Landscape-of-the-State-of-Nagaland.pdf>, (Last visited Jul. 08, 2025).

⁵⁸ Nagaland Population 2025, Sex Ratio, Literacy, <https://www.census2011.co.in/census/state/nagaland.html>, (Last visited May 22, 2025).

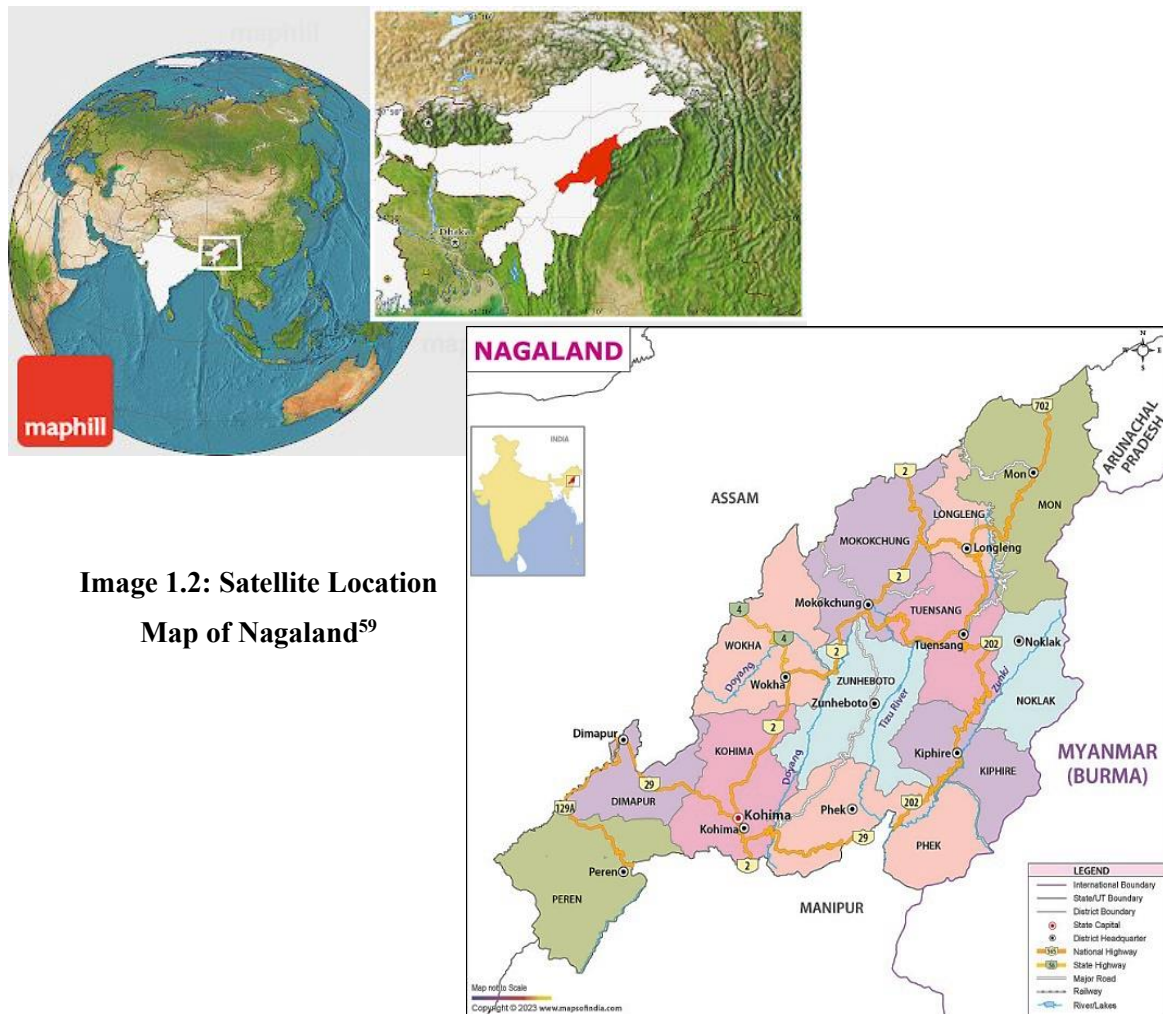


**Image 1.2: Satellite Location
Map of Nagaland⁵⁹**

Image 1.3: Map of Nagaland⁶⁰

The significance of Nagaland in the context of this study lies in its status as a constitutionally autonomous region, where customary law is not merely symbolic but actively governs everyday life. To assess the applicability of the Digital Personal Data Protection Act 2023 in the State of Nagaland, the study adopts a multi-dimensional framework, firstly it undertakes a doctrinal analysis, secondly, it examines the Naga Customary framework focusing on how concepts like privacy, consent, and ownership of information are governed within tribal systems that emphasize collective rights and

⁵⁹ Source of image: <http://www.maphill.com/india/nagaland/location-maps/satellite-map/highlighted-country/>, (Last visited July 05, 2024).

⁶⁰ Source of image: <https://www.mapsofindia.com/maps/nagaland/>, (Last visited July 05, 2024).

community authority, rather than individual autonomy. Laws are not just texts; they must function in a real context, and to supplement this, the study incorporates empirical data gathered through structured questionnaires and interviews. Data are collected from various stakeholders such as students, professionals, Dobashi of the Customary Courts, digital service users and government Officials. Lastly, it evaluates the institutional compatibility between mechanisms envisioned in the Digital Personal Data Protection Act 2023 and Nagaland's existing governance structure. Even if the law is applicable in theory, it must be implementable in practice, through institutions that enjoy legitimacy and trust.

1.5 REVIEW OF LITERATURE

The study seeks to present a comprehensive overview of the major scholarly works undertaken in this field, both globally and within India. The review is systematically classified into two main sections: books and journal articles. Alongside these academic sources, the research also critically examines important judgments delivered by the Supreme Court and various High Courts, as well as key national and international reports, and legal instruments.

1.5.1 Books

1. Apurv Sardeshmukh (Data Protection Law and Regulation)⁶¹ The author analyzes the important provisions with respect to the protection of personal data existing under the current IT Act 2000 and IT Rule 2011. The author discusses the global trends with respect to data protection and discusses the important provisions of the EU GDPR and other data protection regulations across the world.

2. Alessandro Mantelero (Beyond Data Human Rights, Ethical and Social Impact Assessment in AI),⁶² the edited book explores the limitations of existing data

⁶¹ APURV SARDESHMUKH, DATA PROTECTION LAW AND REGULATIONS, Thomson Reuters, first edition 2019.

⁶² 36 ALESSANDRO MANTELERO, BEYOND DATA HUMAN RIGHTS, ETHICAL AND SOCIAL IMPACT ASSESSMENT IN AI, Information Technology and Law Series, Asser Press, <https://link.springer.com/book/10.1007/978-94-6265-531-7>.

protection laws in addressing the ethical and human rights challenges posed by data-driven artificial intelligence (AI). Chapter 1 highlights the need for a more human-centric regulatory approach beyond traditional data protection frameworks. Chapter 2 introduces the Human Rights and Ethical Impact Assessment (HRESIA) model, emphasizing the importance of a structured methodology to evaluate AI's potential human rights impacts. Chapter 3 refines this model through expert-based ethical and societal assessments, while Chapter 4 compares HRESIA with major European AI governance, identifying its strengths in risk management. The book concludes by advocating for proactive, human rights-oriented AI design, focusing on preventive measures rather than post-harm liability mechanisms.

3. Anghrija Chakrabarty, Ashima Obhan and Amar K Sundram (Data Protection Laws Demystified).⁶³ The author of this book provides an insightful and detailed examination of the complexities of data protection laws, particularly within the context of India's Personal Data Protection Bill, 2018. The book traces the evolution of India's data protection regime and offers a comparative analysis with the EU's GDPR, discussing its implications for businesses, individuals, and legal frameworks. It also explores existing Indian legislations such as the Information Technology Act 2005, the Aadhaar Act 2016 and sector-specific data protection measures. The book explains existing and proposed legislation but offers limited critical evaluation of their adequacy in addressing sectoral data protection challenges.

4. Buddhadeb Halder (Privacy in India in the Age of Big Data),⁶⁴ the author critically analyzes the growing privacy challenges in India's digital landscape. It explains that "big data" encompasses not only the vast volume of data but also its velocity and variety. Enormous datasets are generated by government bodies such as UIDAI, Census of India, MGNREGA, and the Income Tax department, as well as through initiatives like Digital India and Smart Cities. Private corporations and non-state actors, including telecom providers and e-commerce platforms, also use such

⁶³ ANGHRIJA CHAKRABARTY, ASHIMA OBHAN AND AMAR K SUNDRAM, DATA PROTECTION LAWS DEMYSTIFIED, Oak Bridge Publications, First Edition (Jan. 1, 2021).

⁶⁴ BUDDHADEB HALDER, PRIVACY IN INDIA IN THE AGE OF BIG DATA, Digital Empowerment Foundation, <https://www.defindia.org/wp-content/uploads/2018/04/Privacy-in-India-in-the-Age-of-Big-Data.pdf>.

data extensively. Despite having privacy policies, most lack effective access controls and clarity over data ownership. The paper highlights the urgent need for a robust legal and ethical framework to safeguard citizens' privacy in the big data era.

5. Dara Hallinan, Ronald Leenes, Serge Gutwirth and Paul De Hert, (Data Protection and Privacy Data Protection and Democracy),⁶⁵ the edited book offers an in-depth exploration of the interplay between democracy, privacy, and data protection. It presents an interdisciplinary perspective on topics such as privacy-by-design, GDPR impact assessments, and e-privacy regulations. Particularly, chapters 2, 5 and 8 are significant for understanding the conceptual and procedural distinction between privacy and data protection, the role of personal data and data controllers, and the balance between open government and individual rights. The author stresses the need for robust legal and governance frameworks to reconcile state security interests with citizens' privacy in democratic societies.

6. Dr Ankita Yadav (Right to Privacy and Data Protection: Special Reference to India)⁶⁶, the author, in her book, explores privacy and data protection as essential principles in the digital era. The author analyzed how increasing technological dependence has led to massive data generation, which can be collected, stored, and used by various entities, citing cases like Facebook and Cambridge Analytica. The book evaluates India's legislative and judicial efforts through Parliament and the Supreme Court to safeguard individual privacy. It further compares India's framework with those of the US and UK, highlighting permissible limitations on privacy rights and emphasizing the crucial role of international treaties in shaping global standards for data protection and privacy preservation.

7. Dr. Harish Kumar Verma et. al. (Personal Data Protection Laws in India),⁶⁷ the book offers a comprehensive examination of the constitutional, judicial, and legal

⁶⁵ 12 DARA HALLINAN, RONALD LEENES, SERGE GUTWIRTH AND PAUL DE HERT, DATA PROTECTION AND PRIVACY DATA PROTECTION AND DEMOCRACY, Oxford: Hart Publishing, 2020.

⁶⁶ DR ANKITA YADAV, RIGHT TO PRIVACY AND DATA PROTECTION: SPECIAL REFERENCE TO INDIA, Satyam Law International, (Apr. 30, 2023).

⁶⁷ DR. HARISH KUMAR VERMA ET. AL., PERSONAL DATA PROTECTION LAWS IN INDIA, Notion Press, 2023.

dimensions of data protection, with a special emphasis on the Indian context. It explores diverse themes, including financial data privacy, matrimonial data protection, and a global perspective on data governance. The book analyses the Digital Personal Data Protection Act 2023, India's first dedicated law on data privacy.

8. D P Mittal (Commentary on the Digital Personal Data Protection Act 2023),⁶⁸

the book provides a clear and accessible interpretation of the Act, enriched with illustrations from Indian and international judicial decisions, including references to the EU's GDPR (2018). It traces the historical evolution of the Digital Personal Data Protection Act 2023, outlining its key features, objectives, and core principles. The author elaborates on essential aspects such as the scope and applicability of the Act, the duties of the data fiduciaries, and the rights of data principals, including consent, correction, erasure, and grievance redressal. The commentary discusses exemptions, lawful processing, state security considerations, and the establishment, powers and appellate functions of the Data Protection Board of India.

9. Kiran Deshta, (Right to Privacy in India under Indian Law),⁶⁹

the book provides an insightful exploration of the evolution and recognition of the right to privacy within the Indian legal framework. It delves into the moral and legal norms of ancient India, highlighting cultural and social practices that reflected early notions of personal privacy. The book presents a comprehensive view of how privacy has developed as both a legal and social value in the Indian context.

10. Luciano Floridi (The Online Manifesto Being Human in a Hyperconnected Era),⁷⁰

the edited book explores how the rise of information and communication technologies has profoundly transformed the human condition. The traditional boundaries between the real and virtual, human and machine, and nature and technology are increasingly blurred, requiring a rethinking of social, ethical, and

⁶⁸ D P MITTAL, COMMENTARY ON THE DIGITAL PERSONAL DATA PROTECTION ACT 2023, Commercial Law Publishers (India) Pvt Ltd, 2024th Edition (Mar. 31, 2024).

⁶⁹ KIRAN DESHTA, RIGHT TO PRIVACY IN INDIA UNDER INDIAN LAW, Deep & Deep Publications (2011).

⁷⁰ LUCIANO FLORIDI, THE ONLINE MANIFESTO BEING HUMAN IN A HYPERCONNECTED ERA, Springer Open, (2015).

political frameworks. It introduces the concept of “*onlife*” experience, a state where the distinction between online and offline ceases to exist. The manifesto calls for reengineering concepts such as privacy, responsibility, and identity to suit a hyperconnected world.

11. Mary C Lacity and Lynda Coon, (Human Privacy in Virtual and Physical Worlds Multidisciplinary Perspectives),⁷¹ The edited book presents a multidisciplinary exploration of privacy, identifying four key themes across its chapters. It defines privacy as a multifaceted and contextual concept that varies across societies and disciplines. The authors discuss the constant tension between individual privacy and collective interests, emphasizing the role of power and regulation in maintaining this balance. Privacy laws such as GDPR, HIPAA and COPPA are examined as essential but minimal safeguards, with advocacy for stronger, proactive privacy measures. The book also explores philosophical, cultural and technological perspectives, drawing parallels between modern digital surveillance and the historical Panopticon model, warning that technological monitoring in the workplace echoes past mechanisms of control and discipline.

12. Navi (Vijayashankar Na), Guardian of Privacy: A Comprehensive Handbook on DPDPA 2023 and DGPSI: Certifiable Audits, Maturity Assessments, and BIS Standards for Data Protection Practitioners in India.⁷² This book serves as a comprehensive and practical guide to India’s evolving data protection frameworks. The book offers an in-depth analysis of the Act’s provisions and implications. It introduces the DGPSI Framework for implementation, a benchmark model integrating the DPDPA 2023, IT Act 2000, and BIS Data Governance standards, providing a certifiable tool for compliance and audit.

⁷¹ MARY C LACITY AND LYNDY COON, HUMAN PRIVACY IN VIRTUAL AND PHYSICAL WORLDS MULTIDISCIPLINARY PERSPECTIVES, Technology, Work and Globalization, (2024).

⁷² NAVI (VIJAYASHANKAR NA), GUARDIAN OF PRIVACY: A COMPREHENSIVE HANDBOOK ON DPDPA 2023 AND DGPSI: CERTIFIABLE AUDITS, MATURITY ASSESSMENTS, AND BIS STANDARDS FOR DATA PROTECTION PRACTITIONERS IN INDIA, Notion Press (Jan. 17, 2024).

13. Puneet Bhasin, (Practical Guide to Digital Personal Data Protection Act, 2023 Law and Compliance),⁷³ the author traces the historical development of privacy law in India and explains the necessity for dedicated data protection legislation. The book provides detailed insights into the provisions of the Digital Personal Data Protection Act, 2023, including its scope, exemptions, enforcement mechanism, and compliance requirements. It serves as a valuable resource for comprehending and implementing India's contemporary data protection regime.

14. Rahul Matthan (The Third Way India's Revolutionary Approach to Data Governance)⁷⁴ The author discusses India's DPI from a governance lens. It describes how, in the hands of a thoughtful regulator, technology can be used to further policy goals. It describes how legal principles could be embedded directly into the fabric of the infrastructure so that the mere act of participating in the ecosystem guarantees compliance. The author first discusses the challenges of data governance in the age of the internet, examining the problems that have arisen because of how data has insinuated itself. The book discussed the range of solutions that comprise the entirety of India's DPI. The final section discusses how India's DPI approach can be used to address the challenges of data governance and analyze India's Data Empowerment and Protection Architecture, which has implemented a consented data sharing framework by directly encoding data protection principles into its workflows.

15. Vijender Kumar Et. Al, (Privacy And Data Protection In The Digital Era)⁷⁵ The book discusses the evolving importance of privacy in today's interconnected world. As the digital age expands, there is a need to safeguard personal data, aligning with the growing significance of privacy as a fundamental right. The book covers the ethical challenges posed by AI, the judicial role in upholding privacy and the complexities of digital footprints. The book examines health data protection, social media, and the vulnerabilities of young gamers.

⁷³ PUNEET BHASIN, PRACTICAL GUIDE TO DIGITAL PERSONAL DATA PROTECTION ACT, 2023 LAW AND COMPLIANCE, OakBridge Publishing, First Edition (Apr. 27, 2024).

⁷⁴ RAHUL MATTHAN, THE THIRD WAY INDIA'S REVOLUTIONARY APPROACH TO DATA GOVERNANCE, Juggernaut Books, (2023).

⁷⁵ VIJENDER KUMAR ET. AL, PRIVACY AND DATA PROTECTION IN THE DIGITAL ERA, Satyam Law International, (2024).

1.5.2 Article

1. Anirudh Burman (Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?)⁷⁶, published by the Carnegie Endowment for International Peace, the author critically analyzes the limitations of India's proposed data protection framework. The paper highlights the excessive discretionary powers granted to the Central government and the Data Protection Authority, which may enable surveillance and weaken privacy protection. The author concluded that India's regulatory capacity constraints demand a narrowly focused law aimed at safeguarding individuals and society from the harms of data misuse, rather than overextending administrative control.

2. A. Shobanadevi et. al. (Novel identity management system using smart blockchain technology).⁷⁷ This paper investigates how blockchain technology can transform identity management and enhance data security. The study examines how blockchain overcomes the shortcomings of traditional identity management systems by granting users complete control over digital identities. These findings demonstrate blockchain's potential to strengthen personal data protection, improve verification mechanisms, and promote efficient, secure data management practices in the digital ecosystem.

3. Charru Malhotra and Udbhav Malhotra (Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India),⁷⁸ the authors critically examine the implications of the DPDP Act for Indian digital citizens. The paper begins by tracing the global evolution of privacy laws in regions such as Singapore, the European Union, and China, before analyzing the origin and key principles of the DPDP Act 2023. The authors assess the Act's effectiveness in striking

⁷⁶ Anirudh Burman, *Will India's Proposed Data Protection Laws Protect Privacy and Promote Growth?*, Carnegie Endowments for International Peace, Mar. 2020, https://carnegie-production-assets.s3.amazonaws.com/static/files/Burman_Data_Privacy.pdf, (Last visited Mar. 03, 2025)

⁷⁷ A. Shobanadevi et. al. *Novel Identity Management System Using Smart Blockchain Technology*, Vol 13, INTERNATIONAL JOURNAL OF SYSTEM ASSURANCE ENGINEERING AND MANAGEMENT, 496-505 (2022), <https://link.springer.com/article/10.1007/s13198-021-01494-0>.

⁷⁸ Charru Malhotra and Udbhav Malhotra, *Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India*, Vol. 70, Issue 3, INDIAN JOURNAL OF PUBLIC ADMINISTRATION, 516-531 (2024), Sage Publications, <https://doi.org/10.1177/00195561241271575>.

a balance between privacy, innovation, and security. They argue that while the Act marks a progressive step, its enforcement needs strengthening and its exceptions must be more precisely defined to ensure comprehensive privacy protection.

4. Diya Sarkar Ghosh, et. al., (The Conundrum of Erasing Digital Footprints: A Regulatory Challenge)⁷⁹, the article explores the growing concerns around individuals' ability to control their digital identities. It examines the "Right to be Forgotten" (RTBF), tracing its evolution from European legal systems to India's emerging data protection regime. The study contrasts Europe's privacy-driven model with America's emphasis on free speech, showing the global divide in managing personal data. In the Indian context, it analyses the Digital Personal Data Protection Act, 2023, which indirectly addresses the right to erasure. The paper highlights regulatory ambiguities, technological challenges, and ethical dilemmas surrounding digital footprint management, emphasizing the need for a balanced framework that safeguards privacy without undermining transparency and data access.

5. Indraves and Dr. Surendra Kalyan (A Review Study to analyze the international Data Protection Frameworks and Best Practices and analyse their applicability and relevance to the Indian Context)⁸⁰ the paper explores the evolution of data protection laws within the framework of India's e-governance initiatives. It examines how international models, particularly the EU's GDPR, influence India's emerging data protection regime. The study emphasizes the constitutional recognition of privacy as a fundamental right under Article 21 and highlights legal instruments such as the IT Act, 2000, and the Personal Data Protection Bill, 2019. It identifies enforcement gaps, transparency issues, and low public awareness as key challenges. The authors recommend legislative reform, stronger enforcement through an independent Data Protection Authority, and enhanced citizen

⁷⁹ Diya Sarkar Ghosh, et. al., *The Conundrum of Erasing Digital Footprints: A Regulatory Challenge*, Vol. 15, JINDAL GLOBAL LAW REVIEW, 25-59 (2024), DOI: <https://doi.org/10.1007/s41020-024-00223-5>.

⁸⁰ Indraves and Dr. Surendra Kalyan, *A Review Study To Analyze The International Data Protection Frameworks And Best Practices And Analyse Their Applicability And Relevance To The Indian Context*, Vol. 2, Issue 1, INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN ARTS, SCIENCE AND TECHNOLOGY, 2024, DOI: <https://doi.org/10.61778/ijmrast.v2i11.96>.

education to ensure a balanced, secure, and privacy-conscious e-governance ecosystem in India.

6. Jane Bambauer, (Is Data Speech?),⁸¹ argues that the collection and sharing of data should be recognized as a form of speech under the First Amendment. She challenges the traditional divide between information gathering and expression, asserting that whenever the state regulates data because it informs or influences people, such regulation should face constitutional scrutiny.

7. Jennifer King and Caroline Meinhardt, (Rethinking Privacy in the AI Era),⁸² the white paper highlights the urgent need to rethink privacy and data protection in the age of artificial intelligence. It argues that existing privacy laws, designed for the internet era, are inadequate to address the complex risks posed by AI, such as data scraping, relational privacy harms, and large-scale surveillance. The authors stress that, as AI development depends on vast data, regulation must prioritize both individual and collective privacy rights. The authors call for stronger transparency, accountability, and data lifecycle governance. Emphasizing human agency, the paper concludes that AI's future is not predetermined; it can and must reflect human values and ethics.

8. Mark J Taylor and Jeannie Marie Paterson (Protecting Privacy in India: The Role of Consent and Fairness in Data Protection),⁸³ the authors critically examine India's data protection frameworks through the lens of consent and fairness. It discusses how the Personal Data Protection Bill 2019 attempts to balance individual autonomy with collective welfare, influenced by Justice Puttaswamy v Union of India. The authors argue that while consent ensures informational self-determination, it is often insufficient in protecting individuals.

⁸¹ Jane Bambauer, *Is Data Speech?*, Vol. 66: 57, STANFORD LAW REVIEW, 2014, https://www.stanfordlawreview.org/wp-content/uploads/sites/3/2014/01/66_Stan._L_Rev_57_Bambauer.pdf.

⁸² Jennifer King and Caroline Meinhardt, *Rethinking Privacy in the AI Era*, Stanford University Human-Centered Artificial Intelligence, White Paper Feb. 2024, <https://hai.stanford.edu/policy/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world>.

⁸³ Mark J Taylor and Jeannie Marie Paterson, *Protecting Privacy in India: The Role of Consent and Fairness in Data Protection*, Vol. 16, Issue 1, INDIAN JOURNAL OF LAW AND TECHNOLOGY, (2020), <https://repository.nls.ac.in/ijlt/vol16/iss1/4>.

9. Paul De Hert, et al. (The right to data portability in the GDPR: Towards user-centric interoperability of digital services)⁸⁴, the authors highlight the right to data portability as a significant step towards developing consumer-focused technologies that enhance data protection and privacy. It empowers individuals to access, transfer, and utilize their personal data, allowing them to benefit from its value within the data-driven economy. Additionally, by promoting data mobility, this right strengthens user autonomy, fosters fair competition among digital service providers, and encourages greater interoperability across technological platforms, thereby supporting a more equitable digital environment.

10. Paulo Camphanha Santana and Faiz Ayat Ansari (Data Protection and Privacy as a Fundamental Right: A Comparative Study of Brazil and India),⁸⁵ the article examines how both nations address the growing challenges of protecting personal data in the digital age. Using an exploratory, comparative approach, the study highlights that data protection and privacy are fundamental but not absolute rights, requiring a balance with public interests like security and law enforcement. Influenced by international standards such as the GDPR, both countries have enacted legislation, India's Digital Personal Data Protection Act and Brazil's LGPD, establishing legal frameworks, principles and regulatory authorities. However, the paper concludes that while these frameworks are promising, their true effectiveness will depend on endorsement, accountability, and institutional strength.

11. Professor Giovanni Sator (The impact of the General Data Protection Regulation (GDPR) on artificial intelligence),⁸⁶ the report examines how the GDPR governs the use of AI and evaluates its suitability within the regulation's conceptual frameworks. It analyzes the relationship between AI operation and core data protection principles such as purpose limitation and data minimization. The study discusses the

⁸⁴ Paul De Hert, et. al, *The Right To Data Portability In The GDPR: Towards User-Centric Interoperability of Digital Services*, Vol. 34, Issue 2, COMPUTER LAW & SECURITY REVIEW, 193-203 (2018), DOI: <https://doi.org/10.1016/j.clsr.2017.10.003>.

⁸⁵ Paulo Camphanha Santana and Faiz Ayat Ansari, *Data Protection and Privacy as a Fundamental Right: A Comparative Study of Brazil and India*, Vol. 9, No. 3, JOURNAL OF LIBERTY AND INTERNATIONAL AFFAIRS, 2023, DOI: <https://doi.org/10.47305/JLIA2393555cs>.

⁸⁶ Professor Giovanni Sator, *The Impact of The General Data Protection Regulation (GDPR) On Artificial Intelligence*, EUROPEAN PARLIAMENTARY RESEARCH SERVICE, June 2020 [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf).

legal grounds for processing of personal data using AI, the obligation to inform individuals about profiling and automated decisions, and the rights of data subjects, including access, erasure and portability. It concludes that although AI can operate in line with GDPR requirements, the regulation needs clear guidance and expanded provisions for effective implementation.

12. Rina Arum Prastyanti and Ridhima Sharma, (Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India)⁸⁷, the article explores how robust data protection frameworks can strengthen consumer confidence in the digital economy. Using a judicial-normative approach, the study compares Indonesia's Personal Data Protection Law and India's Digital Personal Data Protection Act 2023, highlighting their role in safeguarding personal data and fostering trust. It emphasizes that consumer trust depends on the assurance that companies will protect their private information amid growing cybersecurity threats. Despite existing challenges such as weak enforcement and overlapping regulations, the study concludes that effective implementation of data protection laws enhances transparency, reduces privacy risks, and builds competitive advantage for businesses while promoting ethical digital transformation and consumer rights protection in both nations.

13. RK Singh and Vini Singh (Beyond Consent: Ensuring Meaningful Protection of Genetic Data Under India's Digital Personal Data Protection Act, 2023)⁸⁸, the authors critically analyses the adequacy of India's DPDPA in safeguarding genetic data privacy. It highlights that the Act's notice-and-consent model fails to address the unique relational nature of genetic data, which extends beyond individuals to their biological relatives. The authors argue that this model's inadequacy mitigates risks such as discrimination and misuse in law enforcement or employment. They advocate for a harm-based regulatory approach, classifying genetic data according to sensitivity

⁸⁷ Rina Arum Prastyanti and Ridhima Sharma, *Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India*, Vol. 4 No. 2, JOURNAL OF HUMAN RIGHTS, CULTURE AND LEGAL SYSTEM, (2024), DOI: <https://doi.org/10.53955/jhcls.v4i2.200>.

⁸⁸ RK Singh and Vini Singh, *Beyond Consent: Ensuring Meaningful Protection of Genetic Data Under India's Digital Personal Data Protection Act, 2023*, Vol. 46, Issue 4, JOURNAL OF INDIAN ACADEMY OF FORENSIC MEDICINE, 562-567 (2024), DOI: 10.1177/09710973251328785.

and associated risks. The paper proposes reforms, including stronger definitions, privacy-by-design principles, mandatory data protection impact assessments, enhanced grievance redressal, and compensation mechanisms to ensure meaningful protection of genetic information in India's digital ecosystem.

14. Samuel D Warren & Louis D Brandeis (The Right to Privacy)⁸⁹ the foundation work on privacy and protection of personal information, was authored in 1890. This article laid the groundwork for the modern understanding of the right to privacy. The authors were ahead of their time in perceiving how emerging technologies were intruding upon individual privacy. They argued that existing legal principles were inadequate to address these new challenges and emphasized the need for more coherent legal frameworks.

15. Saroj Koul, et. al. (Stakeholders' Understanding of Data Privacy: Implications for Digital Credit Consumers),⁹⁰ paper examines how different stakeholders, digital credit users (DCUs), providers (DCPs), and regulators perceive and implement data privacy in India's digital credit ecosystems. Using a mixed-method approach grounded in Multidimensional Development Theory, the study explores variations in trust, confidence, satisfaction, awareness, and experience regarding data handling practices. It finds that despite the introduction of the Digital Personal Data Protection Act 2023, compliance and enforcement remain inconsistent. Users express concerns about unauthorized data sharing and weak transparency mechanisms. The paper emphasizes the importance of robust regulatory oversight, effective user education, and robust ethical data governance to foster consumer trust, satisfaction, and financial security in India's expanding fintech landscape.

⁸⁹ Samuel D Warren, and Louis D Brandeis, *The Right to Privacy*, Vol 4, No 5, HARVARD LAW REVIEW, 193-220, (1890), <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>.

⁹⁰ Saroj Koul, et. al., *Stakeholders' Understanding of Data Privacy: Implications for Digital Credit Consumers*, Vol. 12, No. 1, COGENT BUSINESS & MANAGEMENT, 2025 DOI: 10.1080/23311975.2025.2568200.

16. Vasudha Khanna and Atul Kotwal (Examining the significance of the Digital Personal Data Protection Act, 2023 in the Context Of The Healthcare Industry: A Comprehensive Analysis),⁹¹ the article provides a detailed analysis of how the DPDP Act reshapes healthcare data governance in India. It highlights the Act's role in ensuring patient privacy, consent-based data processing, and accountability for healthcare providers, insurers, and digital health platforms. The paper examines international parallels, including HIPAA (US), GDPR (UK), PDPA (Singapore), and APPI (Japan), drawing lessons for effective enforcement. It highlights challenges such as technological costs, compliance complexity, and striking a balance between innovation and privacy. The authors conclude that the DPDP Act marks a crucial step toward a privacy-conscious, transparent, and secure digital healthcare ecosystem in India.

1.5.3 Research Gaps

The review of literature highlights significant scholarly contributions in the field of data protection and privacy, both globally and in the Indian context. The research gaps that the researcher has identified are as follows:

- (1) The existing literature extensively discusses the evolution and comparative aspects of data protection laws such as the EU General Data Protection Regulation and India's DPDP Act 2023. However, no scholarly work has yet examined the applicability of these data protection laws within the unique socio-legal context of Nagaland.
- (2) The majority of existing scholarly literature concentrates on the theoretical foundations and legislative dimension of privacy and data protection. However, there is a notable lack of empirical studies into practical aspects such as implementation challenges, institutional capacity, and levels of public awareness, particularly within rural and underdeveloped regions.

⁹¹ Vasudha Khanna and Atul Kotwal, *Examining the significance of the Digital Personal Data Protection Act, 2023 in the Context of The Healthcare Industry: A Comprehensive Analysis*, Vol. 22, DISCOVER PUBLIC HEALTH, (2025), <https://doi.org/10.1186/s12982-025-00757-6>.

- (3) The literature also reveals a gap in understanding the interplay between data protection and indigenous cultural norms, which is crucial for a State with unique customary systems like Nagaland.
- (4) The existing studies predominantly concentrate on sector-specific dimensions without a comprehensive broader administrative, ethical and governance implications of the Digital Personal Data Protection Act 2023 at the regional level.

The research gap lies in connecting national legal provisions with regional realities, particularly in understanding the implementation, governance, and adaptability of data protection laws in Nagaland.

1.6 STATEMENT OF THE PROBLEM

The introduction of the Digital Personal Data Protection Act 2023 marks India's first unified legal response to the growing concerns surrounding personal data, privacy and digital rights. The Act aims to regulate the use of personal data by both state and private entities by introducing principles such as informed consent, purpose limitation, data minimization, and user rights, thereby aligning India's data protection with global standards. However, while its scope appears comprehensive, the Act's enforcement structure assumes a uniformity of digital literacy, institutional capacity, and cultural understanding of privacy that does not hold across India's diverse regional realities. This issue is further influenced by the current level of digital development in Nagaland. According to the Unique Identification Authority of India's Aadhaar Saturation Report dated June 30, 2025⁹², the state has made a notable stride, achieving over 66% Aadhaar saturation, expanding digital banking, and rolling out e-governance services in urban hubs. However, as per the State of India's Digital Economy Report 2024⁹³, published by IPCIDE, ICRIER, Indian Council for Research

⁹² Unique Identification Authority of India, Government of India, *Aadhaar Saturation Report*, Jun. 30, 2025, <https://uidai.gov.in/images/AadhaarSaturationReport.pdf>, (Last visited Jul. 20, 2025).

⁹³ Deepak Mishra, Mansi Kedia et.al, *State of India's Digital Economy (SIDE) Report 2024*, IPCIDE, ICRIER Indian Council for Research on International Economic Relations (ICRIER), Feb. 2024, https://icrier.org/pdf/State_of_India_Digital_Economy_Report_2024.pdf, (Last visited Jul. 20, 2025).

on International Economic Relations (ICRIER), Nagaland ranks among the bottom five Indian states in internet penetration and digital infrastructure access. In such a transitional environment, the imposition of a law that presumes widespread digital access, individual legal awareness and institutional readiness appears disconnected from ground realities.

Moreover, the Digital Personal Data Protection Act 2023 makes no mention of region-specific exemptions or adaptations. The absence of clear guidance on how community-held data, customary knowledge, indigenous knowledge and traditional knowledge and practices should be treated under the law results in legal ambiguity and potential conflicts between statutory obligations and local practices. The core problem, therefore, is not just whether the Digital Personal Data Protection Act 2023 is formally applicable to Nagaland, but whether it is functionally implementable and culturally compatible with the state's unique legal, social and technological environment. And if not,

- *What provisional safeguards are needed to make digital rights truly inclusive?*
- *How should “data rights” be defined in societies where informational control is exercised by customs rather than contract?*
- *What institutional architecture is required to effectively enforce data protection laws and facilitate robust grievance redressal mechanisms?*

1.7 RESEARCH OBJECTIVES

The research objectives are as follows:

- (1) To study the emergence of data protection laws in India, with reference to the judicial developments, regulatory trends and global influences leading up to the enactment of the Digital Personal Data Protection Act 2023.
- (2) To conceptualize the principles of data privacy and the multilayered legal framework governing data protection laws in India, including statutory

provisions, sector-specific regulations, and the institutional mechanisms for enforcement and governance.

- (3) To study global approaches to data privacy and protection, and to evaluate their implications for the development and refinement of India's data protection regime.
- (4) To assess the applicability and enforceability of India's data laws in the State of Nagaland and to identify the administrative, institutional, and infrastructural challenges in implementing the Data Protection Laws within Nagaland.

1.8 SIGNIFICANCE OF THE STUDY

The present study holds great relevance in the contemporary digital era, where the collection, processing and dissemination of personal data have become integral to both governance and business operations. With India rapidly advancing towards a digital economy, the protection of personal data assumes paramount importance. The growing dependence on digital platforms, coupled with increased data generation and exchange, has raised several legal and ethical concerns relating to privacy and misuse of information. In this context, the study assumes significance as it examines the implementation and applicability of India's Digital Personal Data Protection Act, 2023, in the unique socio-legal setting of the State of Nagaland. The study attempts to bridge the gap between legislative intent and practical implementation by assessing the level of awareness, preparedness and compliance among various stakeholders in Nagaland. The study aspires to support the development of a robust and inclusive legal framework that balances technological advancement with the protection of individual privacy. This study highlights the impact of internal diversity and infrastructure on the uniform applicability of the Digital Personal Data Protection Act 2023.

1.9 RESEARCH QUESTIONS

The study is guided by the following key research questions:

- (1) What are the core features, guiding principles, and legal principles underlying the Digital Personal Data Protection Act 2023, and how do they compare with global data protection standards?
- (2) What is the level of awareness and understanding among citizens in Nagaland regarding digital privacy rights, data protection mechanisms, and their responsibilities as data principals?
- (3) Does the existing digital infrastructure in Nagaland support the practical enforcement of the Digital Personal Data Protection Act 2023?
- (4) To what extent do legal, policy and institutional reforms need to be introduced to ensure the effective enforcement of the Digital Personal Data Protection Act 2023, within the socio-legal context of the State of Nagaland?

1.10 HYPOTHESES

This study proceeds on the following hypotheses:

- H1.** The current legal framework governing data protection in India ensures the protection of personal data and the privacy rights of citizens in all states, including Nagaland.
- H2.** The enforcement and implementation of the Digital Personal Data Protection Act 2023 in the State of Nagaland faces significant administrative, infrastructural and institutional challenges due to limited digital readiness and data governance constraints.
- H3.** Awareness of the Digital Personal Data Protection Act 2023, among the citizens in Nagaland, does not differ significantly across age groups.

1.11 RESEARCH METHODOLOGY

The study adopts a mixed-method research design, combining doctrinal legal analysis with empirical socio-legal inquiry to critically examine the evolving framework of data protection in India, with a specific focus on the applicability of the Digital Personal Data Protection Act 2023 to the State of Nagaland. In doctrinal analysis, the researcher has adopted different approaches, such as descriptive, explanatory, analytical, critical and comparative techniques. To explore, interpret, and contrast various legal texts, judicial decisions, and policy frameworks relevant to data protection laws. In addition to the doctrinal analysis, the empirical part of the study incorporated both quantitative and qualitative data. Data was collected through interviews with the key stakeholders and survey questionnaires with the general public who represent various socio-economic sections of the society.

1.11.1 DATA COLLECTION

The data was collected through both primary and secondary sources:

A. Primary Data

i. Questionnaire Schedule

The researcher adopted a questionnaire as the principal tool for gathering primary data. These questions were disseminated through both online and offline modes to ensure broader participation and inclusivity. Structured questionnaires were shared with 400 respondents across four districts, Kohima, Dimapur, Mokokchung and Zunheboto. The survey questionnaire was structured into 6 key dimensions:

Section I: *Demographic profile of the respondents.*

Section II: *Awareness about Data Privacy and Data Protection.*

Section III: *Perception about emerging technology.*

Section IV: *Individual data breach*

Section V: *Perception about Organizational Transparency*

Section VI: *Data Protection in the Nagaland Context*

The questionnaire schedule for the survey, and data collected from the population, have been categorized into the following strata:

1. Students
 - (a) 65 students pursuing a graduate programme and
 - (b) 65 students pursuing a post-graduate programme
2. Academicians (65 respondents)
3. Legal Professionals (65 respondents)
4. Other Professionals (65 respondents)
5. General Public (75 respondents)

ii. Interview Schedule

Semi-structured interviews were conducted with a diverse group of stakeholders. These interviews provided valuable insights into the administrative, sectoral and customary perspectives on data protection and the socio-legal context of Nagaland.

1. District Commissioner (DC): To gain a better understanding of the applicability of the Data Protection Law.
2. Police Headquarters: To gather broader insights on institutional practices and mechanisms related to data protection and cybercrime handling.
3. District Informatics Officer (DIO), National Informatics Centre (NIC): To understand existing data protection practices in government digital systems.
4. Banks and Hospitals: To understand existing data protection practices by Banks and Hospitals.
5. Dobashi of Customary Courts: To learn about the role and perspective of customary legal systems in addressing matters related to data protection and privacy.

B. Secondary Data:

Statutory texts include the Digital Personal Data Protection Act 2023, the Information Technology Act and the Constitution of India. Reports from MeitY, CERT-In, global data protection legislations, reports of international organizations, policy documents, case law, academic literature, and news archives.

1.11.2 SAMPLING DESIGN

To ensure that the empirical component of this study reflects the diversity of digital users across Nagaland, a stratified sampling technique was adopted. The study covers four major districts, Kohima, Dimapur, Zunheboto and Mokokchung. The total population across these districts, as per the 2011 census report⁹⁴, stands at 9,82,178, distributed as Kohima (2,67,988), Dimapur (3,78,811), Zunheboto (1,40,757) and Mokokchung (1,94,622).

Where the sample size is calculated using Taro Yaman's Formula.⁹⁵

$$\begin{aligned} n &= \frac{N}{K+N(e)^2} \\ &= \frac{982178}{1+982178(0.05)^2} \\ &= \frac{982178}{1+ 982178 (0.00250000000000000005)} \end{aligned}$$

Where,
n = is the sample size
N = is the total population size
e = is the margin of error
K = is constant (1)

n = 400 (Total sample size is 400)

The total population surveyed is 400, proportionally distributed across four key districts of Nagaland. The sampling was based on stratified purposive sampling, ensuring that key demographic and professional groups were represented. The distribution is as follows:

⁹⁴ <https://www.census2011.co.in/census/state/districtlist/nagaland.html>, (Last visited July 05, 2024).

⁹⁵ <https://dissertationdataanalysishelp.com/sample-size-calculator/>, (Last visited July 05, 2024).

Table 1.1: Distribution of respondents

District	Population	% of total Population	Sample Size
Dimapur	3,78,811	38.57%	154
Kohima	2,67,988	27.29%	109
Mokokchung	1,94,622	19.82%	80
Zunheboto	1,40,757	14.33%	57
Total=			400

1.11.3 TABULATION, ANALYSIS AND PRESENTATION

The data collected through the survey and interview are systematically tabulated to ensure clarity, accuracy, and ease of interpretation. Quantitative data are numerically coded and entered into IBM SPSS version 25 software and MS Excel for analysis.

i. Coding Scheme: The responses were numerically coded for consistency and accurate statistical analysis, and interpretation:

- (a) **Dichotomous scale:**
No = 1
Yes = 2
- (b) **Trichotomous scale:**
No = 1
Maybe = 2
Yes = 3
- (c) **5-point Likert Scale:**
Strongly disagree = 1
Disagree = 2
Neutral = 3
Agree = 4
Strongly agree = 5
- (d) **5-point Likert Scale:**
Never = 1
Rarely = 2
Sometimes = 3
Often = 4
Always = 5

- (e) **4-point Likert Scale:** Never = 1
Rarely = 2
Occasionally = 3
Frequently = 4
- (f) **Rating scale 1 to 5:** 1 = Very ineffective
2 = Ineffective
3 = Moderately
4 = effective
5 = Highly effective

ii. Tools and Techniques: Qualitative data from semi-structured interviews are thematically coded to complement quantitative findings. Findings are presented through a combination of bar charts, pie graphs, histograms and tabular summaries. The following tools and techniques were used:

- Descriptive statistics (frequencies, means, percentages) for awareness and behaviour-based responses.
- Cross-tabulation to compare practices across age groups and professions.
- Chi-Square Independence Test to test whether there is any significant relationship between two variables.
- Kruskal-Wallis Test to compare independent groups to determine if there are statistically significant differences between them.
- P-value (< 0.05) is used to evaluate if the observed differences are statistically significant.

iii. Ethical considerations: The study strictly adhered to established ethical standards by maintaining the confidentiality and anonymity of participants, obtaining informed consent, and ensuring that all data were collected, stored, and used responsibly.

1.12 LIMITATIONS OF THE STUDY

While the study attempts to provide a comprehensive and context-sensitive understanding of the Digital Personal Data Protection Act's applicability in Nagaland, certain inherent limitations are:

1. The Digital Personal Data Protection Act was enacted in 2023, but the Act had not yet come into force as of 2025. The study focuses on the pre-enforcement context; it relies on anticipatory analysis rather than post-implementation outcomes.
2. A major limitation is that this study considers personal data as defined under the DPDP Act 2023. Non-personal data are excluded from the scope of this study.
3. The field study was confined to four districts of Nagaland (Kohima, Dimapur, Mokokchung and Zunheboto). These districts were purposefully chosen to represent administrative, commercial, and socio-cultural diversity. The findings may not entirely reflect the realities of other districts within the state.

1.13 SCHEME OF CHAPTERIZATION

The study is divided into seven chapters. They are as follows

Chapter 1: Introduction- Chapter 1 is the introduction to the thesis. It includes the legal development of data privacy, defines key terms, research problems, objectives, hypotheses and research questions. The chapter outlines the significance, scope and limitations of the study, along with the data collection and sampling techniques.

Chapter 2: Genesis of Data Protection Laws in India – This chapter examines the historical and legislative evolution of data protection in India, spanning from the early regulatory measures under the India Telegraph Act of 1885 to the rapid legal development in the post-independence period. It covers major milestones such as the Information Technology Act 2000 and its amendments, Information Technology Rules 2011 and 2021. The chapter further analyses the contribution of the expert

committee's report and the evolution of successive data protection bills, resulting in the enactment of the Digital Personal Data Protection Act 2023 and also discusses the Nagaland State Data Sharing and Accessibility Policy 2024.

Chapter 3: Conceptual Foundation and Multilayered Legal Frameworks on Data Protection in India- This chapter 3 is structured into three parts to present data protection laws in India. Part I- Data privacy conceptual framework explains the nature, classifications, and characteristics of data. Part II, multilayered legal regulatory frameworks, reviews constitutional provisions, the Digital Personal Data Protection Act 2023, other statutory laws, sector-specific regulations and ethical guidelines governing data use. Part III examines the role of key institutional architecture for Data Governance in India.

Chapter 4: International Legal Frameworks on Data Privacy and Data Protection – This chapter examines the international legal frameworks governing data privacy and data protection, including the evolution of norms from early development to the transition from soft law to binding treaties, as well as the influence of digitalization and cross-border data flows. It covers key international instruments, such as Convention 108+, the APEC Privacy Framework, OECD Guidelines, and UN initiatives. Further, this chapter also discusses the regional approach to data privacy, such as the EU's GDPR 2018, California Privacy Rights Act 2020, Canada's PIPEDA 2000, South Africa's POPIA Act 2013, South Korea's PIPA 2011 and neighbouring country China's PIPL 2021.

Chapter 5: Critical Appraisal of the Digital Personal Data Protection Act 2023 - This chapter critically analyses the Act in key dimensions, such as the legal philosophy of data privacy within India, gaps in the legal structure, cross-border data transfer mechanisms, extensive surveillance and state exemptions, inadequate safeguards for algorithmic governance and automated decision-making, data fiduciary duties and accountability. The chapter further addresses the Act's regulatory silence on emerging technologies, such as artificial intelligence, the Internet of Things, and blockchain technology. Concerns related to data localization and inadequate data breach notification protocols. Lastly, a comparative study with global legislation to

strengthen institutional design and enhance technological adaptability in India's data protection regime.

Chapter 6: Assessing the Applicability of Data Protection Laws in the State of Nagaland: An Analysis- This chapter examines the extent to which data protection laws are applicable and effective in the State of Nagaland. It undertakes both doctrinal and empirical analysis to understand the alignment between statutory provisions and their practical implementation. The doctrinal study focuses on the legal frameworks, and the empirical part explores the awareness, compliance, and enforcement mechanisms within the state. Through this dual approach, the chapter seeks to assess whether existing data protection norms adequately address the unique socio-legal realities of Nagaland.

Chapter 7: Findings, Conclusion and Suggestions – This chapter presents the key findings of the study, drawing together the conceptual analysis and empirical evidence to present an integrated understanding of the research problem. It reflects on the extent to which the research objectives have been achieved, assessing the implications of the findings for data protection and privacy governance. Based on the analysis, the chapter proposes a set of suggestions aimed at addressing identified gaps and aligning the legal framework with evolving technological and societal needs.

CHAPTER - 2

GENESIS OF DATA PROTECTION LAWS IN INDIA

2.1 INTRODUCTION

In today's digital age, protecting personal data is a critical concern, affecting individual privacy, businesses, and governments' functioning. The genesis of data protection laws in India reflects a broader global movement toward regulating the flow and protection of personal data in response to technological advancements, with significant implications for individual rights and national security. The digital revolution has fundamentally altered how personal data is collected, processed, and stored, leading to growing concerns over privacy, security, and data misuse. As individuals, businesses, and governments increasingly rely on digital platforms for everything from commerce to governance, protecting personal data has become a critical issue worldwide. Global trends, judicial interventions, and the rising importance of data in economic and governance structures have shaped India's journey towards establishing data protection laws. In India, the evolving digital ecosystem has prompted the development of comprehensive data protection laws aimed at safeguarding the privacy and personal information of its citizens. Additionally, the rise of the digital economy transformed how personal data was collected, processed, and utilized. Data has become a valuable asset with sectors like e-commerce, digital payments, and social media witnessing exponential growth. This digital revolution not only amplified the risk of data misuse but also highlighted the need for a legal framework to ensure privacy and security without stifling innovation. Together, these factors laid the groundwork for India's journey toward establishing robust data protection laws.

India's journey toward establishing a formal data protection regime began with the Information Technology Act 2000, which addressed cybersecurity and data breaches but lacked a comprehensive framework for protecting personal data. The need for robust data protection laws gained momentum after the landmark Supreme

Court ruling in 2017 in the *Justice K.S. Puttaswamy v. Union of India*⁹⁶ case, which recognized the Right to Privacy as a fundamental right under the Constitution of India. This judgment has catalyzed the drafting of the Personal Data Protection Bill, later evolving into the Digital Personal Data Protection Act, 2023, a law designed to regulate the collection, storage, and processing of personal data, ensuring that individuals have control over their personal information. The enforcement of data protection laws in India has been a complex task, primarily due to the rapid pace of technological evolution. Innovations such as artificial intelligence, the Internet of Things (IoT), and big data analytics continue to be effective. Laws that may seem adequate risk become obsolete in the face of unforeseen technological advancement, creating a constant need for adaptive and forward-looking regulatory frameworks. India's diverse socio-economic and technological landscape adds another layer of complexity. With a vast population spread across urban and rural regions, varying levels of digital literacy, and uneven access to technology, implementing a uniform data protection framework poses significant challenges. While urban areas may adapt relatively quickly to stricter data regulations, rural regions, where digital penetration and awareness are lower, may struggle with compliance. Additionally, smaller businesses and startups may find it burdensome to meet stringent data protection requirements, potentially stifling innovation and growth in an already competitive market.

Balancing the right to privacy with national security and economic innovation remains one of the most contentious aspects. On the one hand, robust data protection laws are essential for upholding individual privacy and ensuring trust in digital systems. On the other hand, government and security agencies argue for access to data to combat terrorism, cybercrime, and other national threats. Striking a balance between these competing priorities requires a nuanced approach that respects constitutional rights while addressing legitimate security concerns. Moreover, fostering innovation in India's growing digital economy demands flexible regulations and is conducive to technological progress. These challenges highlight the intricate balancing act required to design and implement effective data protection laws in India.

⁹⁶ Justice K S Puttaswamy (Retd) & Anr. Vs Union of India & Ors. (2017) 10 SCC 1

2.2 EMERGENCE OF DATA PROTECTION LAWS IN INDIA

Data has emerged as a valuable asset in the digital age, often called the new oil. Meglena Kuneva, European Consumer Commissioner and keynote speaker at the Roundtable on Online Data Collection, Targeting and Profiling, emphasized that *“Personal data is the new oil of the Internet and the new currency of the digital world⁹⁷.”* The proliferation of the internet, the expansion of online services, and the surge in personal data exchanges have underscored the need for robust data protection mechanisms. Like many nations, India has recognized the importance of safeguarding personal data and addressing privacy concerns. The journey towards establishing a comprehensive legal framework for data protection in India has been a long and evolving process, culminating in the enactment of the Digital Personal Data Protection Act 2023. Technological advancements, global trends, judicial interventions, and the growing importance of personal data in the digital age have shaped the evolution of data protection laws in India. Historically, India’s legal framework on privacy and data protection was fragmented, primarily covering specific aspects of electronic communication and cybersecurity. Over time, the need for a comprehensive data protection law became apparent, particularly with the rise of the internet, social media, and digital services. This historical journey can be traced from colonial laws to modern-day legislation, reflecting the broader socio-political changes in the country. These include various data protection bills, committee reports, and judicial push that reflect India's journey towards establishing a comprehensive legal framework for data privacy and protection in the digital age.

2.2.1 Early Beginnings: Pre-Independent India

The concept of data protection, as we understand it today, was not explicitly recognized in the early legal framework of colonial India. In colonial India, privacy as a legal right was not recognized. However, certain laws and legal principles laid a foundational framework for privacy and protection of information, which indirectly contributed to the evolution of data protection laws in post-independence India. For

⁹⁷ Meglena Kuneva, European Consumer Commissioner, March 2009, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156, (Last visited Dec. 03, 2024).

example, the *Indian Evidence Act 1872*⁹⁸ includes provisions that safeguard sensitive information in judicial proceedings, particularly through section 123⁹⁹, which prohibits the disclosure of evidence derived from unpublished official records concerning state affairs unless authorized by the head of the respective department, who has full discretion to grant or deny such permission. Similarly, section 124¹⁰⁰ of the Indian Evidence Act 1872 ensures that public officers are not obligated to reveal communications made to them in official confidence if they determine that doing so would compromise public interest. These sections highlight an early recognition of the importance of protecting confidential information while striking a balance between transparency and state security.

(a) *The Indian Telegraph Act 1885*

The Indian Telegraph Act 1885¹⁰¹ does not have explicit provisions for data protection, as it was designed in a pre-digital era to regulate telegraphy and communications. Its focus is primarily on control, interception, and communication monitoring for state purposes rather than safeguarding individual data or privacy. The pre-independence legal framework in India did not explicitly address data privacy; it established principles related to confidentiality, state control, and limited individual protections. These laws reflected the priorities of a colonial administration focused on governance and surveillance rather than individual rights. The Act allows the government to intercept or detain messages in cases of public emergency or public safety; however,

- (i) it does not specify safeguards for protecting the intercepted data,
- (ii) there are no requirements for securing this data against misuse or unauthorized access, and

⁹⁸ The Indian Evidence Act, 1872, (No 1), Act of Parliament, 1872 (India).

⁹⁹ The Indian Evidence Act, 1872, (No 1) § 123. Evidence as to affairs of State.- No one shall be permitted to give any evidence derived from unpublished official records relating to any affairs of State, except with the permission of the officer at the head of the department concerned, who shall give or withhold such permission as he thinks fit.

¹⁰⁰ The Indian Evidence Act, 1872, (No 1) § 124 official communications.- No public officer shall be compelled to disclose communications made to him in official confidence when he considers that the public interests would suffer by the disclosure.

¹⁰¹ The Indian Telegraph Act, 1885 (No. 13), Act of Parliament, 1885 (India).

(iii) It lacks provisions for a data retention limit (section 5 (2))¹⁰² of the Act).

2.2.2 Post-Independence Era (1947–2000)

The Constitutional Context (1950s): After independence, India adopted the Constitution in 1950, which guaranteed fundamental rights, including the Right to Life and Personal Liberty under Article 21. However, privacy was not explicitly recognized as a fundamental right in the original Constitution. During this time, courts began interpreting personal liberty more broadly, laying the groundwork for privacy jurisprudence. The Constitutional right to privacy was developed in the 1950s in the milieu of police supervision of the accused and domiciliary visits to a person's home at midnight. In the case of *M.P. Sharma v. Satish Chandra*¹⁰³, the Supreme Court held that, even though search and seizure is a part of the responsibilities of a police officer, such act at midnight is a violation of Article 19(1) (f)¹⁰⁴ of the Constitution. The Court added that a mere search by a police officer did not affect any property right, and the seizure related to it was just temporary and did not violate the right to privacy, as the Constitution of India did not have the fundamental right to privacy analogous to that of the Fourth Amendment of the US Constitution¹⁰⁵. Later, in the case of *Kharak Singh v. State of Uttar Pradesh*¹⁰⁶ (1963), the court held that the right to liberty comes under Art. 21. The Supreme Court started to acknowledge the concept of privacy, albeit in limited terms, linked to physical privacy rather than informational privacy. Similarly, in the case of *Pooran Mal v Director of Inspection (Investigation)*

¹⁰² The Indian Telegraph Act, 1885 (No 13) § 5 (2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign State or public order or for preventing incitement to the commission of an offence, for reason to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order: Provided that press message intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section.

¹⁰³ *M.P Sharma v. Satish Chandra* (1954) 1 SCR 1077.

¹⁰⁴ INDIA CONSTITUTION art. 19(1)(f)- All citizens shall have the right to acquire, hold and dispose of property. The right to property is omitted by the Constitution (forty-fourth Amendment) Act, 1978.

¹⁰⁵ <https://privacylibrary.ccgnlud.org/case/saroj-rani-vs-sudarshan-kumar-chadha>.

¹⁰⁶ *Kharak Singh v. State of Uttar Pradesh*- AIR 1963 SC 1295.

of *Income-Tax, New Delhi*¹⁰⁷, the court categorically states that searches done by the government body to gather evidence would not be a violation, as there is no fundamental right to privacy. In the case of *Govind v State of Madhya Pradesh*¹⁰⁸ privacy issue was brought before the Supreme Court, where the petitioner argued that certain police actions violated his right to privacy. In this case, the court faces the challenge of defining whether privacy could be considered a fundamental right under the Constitution. The court observed that the right to privacy can only be denied if the public interest outweighs privacy. Any law that limits privacy “*must satisfy the compelling state interest test*”. Justice Mathew stated that

*“Rights and freedoms of citizens are set forth in the Constitution in order’ to guarantee that the individual, his personality and those things stamped. With his personality shall be free from official interference except where a reasonable basis for intrusion exists. ‘Liberty against government’ a phrase coined by Professor Corwin expresses this idea forcefully. In this sense, many of the fundamental rights of citizens can be described as contributing to the right to privacy”*¹⁰⁹

In *R Rajagopal v. State of Tamil Nadu*¹¹⁰ the petitioner was an editor, printer and publisher of a Tamil weekly magazine published in Tamil Nadu who wanted an order limiting the State of Tamil Nadu from snooping with the authorized publication of the autobiography of Auto Shankar, a prisoner awaiting the death penalty. Later, in another case, Justice. Jeevan Reddy explicitly mentioned that the right to privacy is implicit in Articles 21 and 19 of the Indian Constitution.

(a) Late 1980s Legal Development

The evolution of data security in India began in the late 1980s when General Electric (GE) pioneered outsourcing operations, laying the foundation for India’s position as

¹⁰⁷ Pooran Mal v Director of Inspection (Investigation) of Income-Tax, New Delhi- AIR 1974 SC 348

¹⁰⁸ Govind v State of Madhya Pradesh- 1975 AIR 1378.

¹⁰⁹ Govind v State of Madhya Pradesh- 1975 AIR 1378- Judgment page no 9, <https://api.sci.gov.in/jonew/judis/6014.pdf> (Last visited Dec. 03, 2024).

¹¹⁰ R Rajagopal v. State of Tamil Nadu- AIR 1995 SC 264.

a global outsourcing hub.¹¹¹ General Electric's collaboration with Wipro Ltd in 1989 marked the beginning of cross-border business process outsourcing (BPO), primarily focusing on data entry, credit card processing, and customer services¹¹². In September 1989, Jack Welch, who was the Chairman and CEO of GE, held a meeting with the Chief Technical Advisor to Prime Minister Rajiv Gandhi. During their discussion, the advisor convinced Mr Welch about the potential opportunities for GE in India. As a result of the meeting, General Electric partnered with Wipro Ltd through a joint venture to develop and market medical equipment in India¹¹³. India's restrictive foreign investment policies before 1991 limited economic opportunities. However, this changed under Dr Manmohan Singh, then Finance Minister, whose liberalization policies attracted foreign investors, especially in the telecom sector. Flexible regulations led to the installation of satellite downlink stations, which improved connectivity and made India an attractive destination for numerous American multinational corporations, including Citigroup, Microsoft, Delta Airlines, IBM, Accenture, and many others, which have established outsourcing partnerships with prominent Indian companies like Infosys Technologies, Wipro, Mphasis, and Tata Consulting.

Outsourcing services began in India in the 1980s and experienced significant growth during the 1990s. In the modern era, where information technology plays a vital role in business operations, the concept of outsourcing has evolved drastically over time¹¹⁴. As per the findings from a study on the BPO sector in Gurgaon by Manish Vaid the number of professionals employed in India's information technology and ITES-BPO sectors grew from 2,84,000 in 1999-2000 to over 1.6 million by 2006-

¹¹¹ General Electric was one of the first American Companies to take advantage of outsourcing opportunities in India.

¹¹² George Barbara Crutchfield and Gaut Deorah Roach, *Offshore Outsourcing To India By U.S. And E.U. Companies Legal And Cross-Cultural Issues That Affect Data Privacy Regulation In Business Process Outsourcing*, BUSINESS LAW JOURNAL, 6 U.C Davis Bus. L.J 13 (2006), <https://pavanduggal.com/wp-content/uploads/2016/01/Offshore-Outsourcing-to-India-by-U.S.-and-E.U.-Companies-Legal-and-Cross-Cultural-Issues-that-Affect-Data-Privacy-Regulation-in-Business-Process-Outsourcing.pdf> (Last visited Dec. 02, 2024).

¹¹³ Ibid.

¹¹⁴ *The Outsourcing History of India*, Outsource2india, <https://www.outsource2india.com/why-india/articles/the-outsourcing-history-of-india.asp#:~:text=Services%20outsourcing%20to%20India%20started,drastic%20change%20over%20the%20years>, (Last visited Dec. 06, 2024).

2007 with 70% of the workforce aged between 26-35 years, the IT-ITES industry is poised to become one the largest employers of young adults in the country. Currently, Bangalore, Mumbai, the National Capital Region (NCR), Hyderabad, Pune, Chennai and Kolkata together contribute 90% of total direct employment in the BPO sector¹¹⁵. The growth of outsourcing raised concerns about data security, as sensitive personal information, such as credit card details, medical records, and social security numbers, became more accessible. Indian employees in BPOs handle critical customer data through various services like tax preparation, credit card processing, and help desk support. This growth has also amplified the need for robust data protection mechanisms to safeguard personal information.

2.3 INITIAL LEGAL FRAMEWORKS IN INDIA (From 2000- 2011)

The transfer of sensitive personal information poses a significant risk, as US federal laws do not extend to foreign companies operating abroad. As a result, numerous BPO services in India have proactively implemented voluntary controls, including self-regulation, and have adopted strict security measures to minimize the risks associated with the misuse of confidential personal data. Apart from this, during the late 1990s, there was an effort to integrate data privacy protection into India's proposed information technology legislation. Prime Minister Atal Bihari Vajpayee emphasized the urgent need for formulating a comprehensive action plan. As a first step in this direction, a high-level National Task Force on IT and Software Development was established on May 22, 1998, under the Chairmanship of the Deputy Chairman of the Planning Commission Shri. Jaswant Singh, co-chaired by Shri. N Chandrababu Naidu, Chief Minister of Andhra Pradesh and Dr M. G. K. Menon, former Minister of State for Science and Technology. Its members include eminent representatives from the Government, industry and academia¹¹⁶.

¹¹⁵ Vaid, Monisha, *Exploring the lives of youth in the BPO sector: Findings from a study in Gurgaon*, Health and Population Innovation Fellowship Programme Working Paper no. 10. (2009), Population Council, https://knowledgecommons.popcouncil.org/cgi/viewcontent.cgi?article=1509&context=departments_sbsr-rh (Last visited Dec. 06, 2024).

¹¹⁶ The Information Technology Action Plan 1998, <https://indiancabletv.net/itplan.htm#pre> (Last visited Dec. 03, 2024).

The National Task Force on IT and Software Development was established by the Government of India to promote and accelerate the development of the information technology (IT) and software sectors in the country. Its primary purpose was to create a policy framework, recommend strategic initiatives and address challenges to transform India into a global leader in IT and software development. The key objectives are to promote IT industry Growth, boost employment, formulate policy frameworks, enhance infrastructure, encourage education and skill development, promote e-governance, attract investments, collaborate with stakeholders and address cybersecurity. The National Task Force on IT and Software Development submitted an “*Information Technology Action Plan*” (Plan) to the Prime Minister on July 4, 1998, which contains 108 recommendations covering both bottleneck areas and broad promotional measures that are crucial for boosting IT in India. The basic objectives are (i) Info-Infrastructure Drive, (ii) Target ITEX-50 and (iii) IT for all by 2008. The recommendations outlined in points 104¹¹⁷ and 107¹¹⁸ reflect a forward-thinking approach to strengthening India’s cybersecurity landscape and digital governance. Recommendation 104 focuses on the strategic transfer of cryptology and cybersecurity expertise from the defense establishment to civilian information security agencies. This collaboration aims to enhance national information security and network protection while fostering a secure digital environment for the use of technologies like electronic fund transfer and digital signatures. Recommendation 107 complements this by advocating for the rapid approval and implementation of cyber laws.

These two recommendations underscore the need for a synchronized effort between leveraging specialized expertise and establishing enforceable legal structures. However, this initiative only partially materialized with the enactment of

¹¹⁷ The Information Technology Action Plan – Recommendation 104- The cryptology and Cyber Security knowledge and experience developed by the Defence establishment shall be suitably transferred to the civilian information security agencies for wider dissemination in the country to increase information security, network security and bring about a greater degree of secure use of EFT, Digital signature, etc. <https://indiancabletv.net/itplan.htm#pre>.

¹¹⁸ The Information Technology Action Plan – Recommendation 107- The draft set of Cyber Laws prepared by the Cyber Law Committee of Secretariates, shall be approved by the Government with suitable modifications and implemented, as a first step, within six months, available at: <https://indiancabletv.net/itplan.htm#pre>.

the Indian Information Technology Act 2000. While the Act addresses issues like unauthorized access and data theft from computers and networks, it falls short of adequately addressing privacy and data protection concerns. Apart from this, the judgment of the *People's Union for Civil Liberties (PUCL) v. Union of India*¹¹⁹ (1997) raised concerns about telephone tapping and surveillance, highlighting the growing need for a legal framework to protect personal information in the digital age.

2.3.1 The Information Technology Act 2000

The initial response to concerns about data protection was the Information Technology Act 2000¹²⁰. The Act provides legal recognition for transactions conducted through electronic data interchange and electronic communication, commonly known as “*electronic commerce*”¹²¹. The Act specifies that any unauthorized downloading, copying, or extraction of data, computer database, or information from a computer, system, or network can result in liability to pay damages¹²². Before the enactment of a dedicated data protection law in India, the legal foundation for regulating digital data was primarily established through the Information Technology Act, 2000, and its accompanying rules (2011 and 2021). Criminal offences recognized under the Act include tampering with computer source documents, hacking into computer systems, and publishing obscene content in electronic form. However, the Act does not clearly define or regulate the collection, storage, and processing of personal data by private or public entities, leaving significant gaps in user privacy safeguards. For instance, Section 43A¹²³ of the IT Act mandated compensation for failure to protect data, and

¹¹⁹ People's Union for Civil Liberties (PUCL) v. Union of India- AIR 1997 SC 568.

¹²⁰ The Information Technology Act 2000, (No 21) Act of Parliament, 2000 (India).

¹²¹ Electronic Commerce- legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication which involves the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies.

¹²² The Information Technology Act 2000, (No 21) § 43. Penalty and Compensation for damage to computer, computer systems, etc.

¹²³ The Information Technology Act 2000, (No 21) § 43A- 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 person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. (Ins by s 22 w.e.f. 27-10-2009).

Section 72¹²⁴ penalized breaches of confidentiality. However, these provisions were limited in scope, dealing mainly with cybersecurity and focusing on specific instances of misuse, rather than creating a comprehensive data protection framework. However, in the absence of dedicated data protection legislation, the Act became a de facto data privacy law, albeit by accident more than design. Information Technology Rule 2011 marked India's first formal recognition of personal and sensitive data. These were further extended by the National Cyber Security Policy and IT Rule 2021; together, these instruments have served as India's interim data protection frameworks. Thus, the Information Technology Act laid the groundwork for cyber regulation in India.

2.3.2 The Credit Information Companies (Regulation) Act 2005

The Credit Information Companies (Regulation) Act, 2005¹²⁵ (CICRA) was enacted to regulate credit information companies in India, ensuring the efficient collection, processing and sharing of credit-related information. They set limits on who can access the data, how it can be used, and how long it can be stored, ensuring transparency and reducing the risk of misuse. The Act restricts the use of credit data to specific purposes, such as evaluating creditworthiness, and mandates periodic checks to ensure the information's accuracy. It further regulates the storage of credit information by setting rules for its retention, deletion, and record-keeping. Additionally, the Reserve Bank of India (RBI) holds the authority to introduce further guidelines to ensure these principles are effectively implemented. Specified users, such as lenders and other authorized entities, must also adhere to strict guidelines for recording, preserving and protecting credit information to prevent unauthorized access or misuse. Electronic networking among CICs, credit institutions, and users is encouraged to streamline operations while maintaining security. The Privacy Principles in the Credit Information Companies (Regulation) Act, 2005, were

¹²⁴ The Information Technology Act 2000, (No 21) § 72- Penalty for Breach of Confidentiality and Privacy- Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other materials without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other materials to any other person shall be [liable to penalty which may extend to five lakh rupees].

¹²⁵ The Credit Information Companies (Regulation) Act 2005, (No 30), Act of Parliament, (India).

discussed under the provisions of Section 20¹²⁶ of the Act, establishing a comprehensive framework for the responsible handling of credit data by credit information companies, credit institutions, and specified users. These principles ensure that data collection, processing and sharing are carried out with clear rules to safeguard individual privacy. For instance, credit institutions are required to collect information from borrowers responsibly, ensuring accuracy and transparency in the data provided to CICs. As per the provisions of Section 23(2)¹²⁷, every credit information company, credit institution or specified users who willfully commit any act or engage in any practice violating the principles of Section 20 of the Act shall be subject to a fine not exceeding one crore rupees. These measures collectively aim to protect the privacy of individuals while promoting a secure and transparent credit ecosystem.

¹²⁶ The Credit Information Companies (Regulation) Act 2005, (No 30) § 20- Privacy Principles.- Every credit information company, credit institution and specified user, shall adopt the following privacy principles in relation to collection, processing, collating, recording, preserving, 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; (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 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) for any principles and procedures relating to credit information which the Reserve Bank may consider necessary and appropriate and may be specified by regulations.

¹²⁷ The Credit Information Companies (Regulation) Act 2005, (No 30) § 23. Offences and penalties- (2) every credit information company or credit institution or any specified users, willfully, performing any act or engaging in any practices, in breach of any of the principles referred to in section 20, shall be punishable with fine not exceeding one crore rupees.

2.3.3 The Information Technology (Amendment) Act 2008

The IT Amendment Act of 2008 ¹²⁸ marked a significant step in strengthening India's cybersecurity framework, particularly addressing the growing challenges of cybercrimes. There has been a lot of focus on IT because of recent developments nationally and internationally, particularly w.r.t provisions related to data protection and privacy in the context of BPO operations, liability of network service providers, computer-related offences, regulation of cyber cafes, etc. ¹²⁹ The recent concerns about the operating provisions in the IT Act related to "*Data Protection and Privacy*", in addition to contractual agreements between the parties, the existing Sections 43, 66, 69 and 72 have been revisited, and some amendments have been provided. These are:

- (i) Section 43(A)¹³⁰ related to the handling of sensitive personal data or information with reasonable security practices and procedures thereto.
- (ii) Gradation of severity of computer-related offences under Section 66¹³¹, committed dishonestly or fraudulently, and the punishment thereof.
- (iii) Proposed additional Section 72(A)¹³² punishment for disclosure of information in breach of a lawful contract.
- (iv) Surveillance power to the government through Section 69¹³³.

¹²⁸ The Information Technology (Amendment) Act 2008, (No 10), Act of Parliament, 2008 (India).

¹²⁹ Expert Committee Report on Amendments to IT Act 2000, Press Information Bureau, August 29, 2005, <https://www.meity.gov.in/content/report-expert-committee-amendments-it-act-2000>.

¹³⁰ The Information Technology Act 2000, (No 21) § 43A-Compensation for failure to protect data.- Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resources 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 person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

¹³¹ The Information Technology Act 2000, (No 21) § 66- Computer-related Offences, § 66A- Punishment for sending offensive messages through communication services, § 66B- Punishment for dishonestly receiving stolen computer resource or communication devices. § 66C- Punishment for identity theft. § 66D- Punishment for cheating by personation by using computer resources. § 66E- Punishment for violation of privacy and § 66F- Punishment for Cyber Terrorism.

¹³² The Information Technology Act 2000, (No 21) § 72A- Punishment for disclosure of information in breach of lawful contract- 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. (Inserted by section 37 of the IT Amendment Act 2008, w.e.f. 27-10-2009).

¹³³ The Information Technology Act 2000, (No 21) § 69- Power to issue directions for interception or monitoring or decryption of any information through any computer resources.

Following the 26/11 Mumbai Attacks, the amendment introduced the concept of cyber terrorism and imposed stringent punishment for it. The scope of cybercrime under Section 66 was expanded with several significant additions that defined various cyber offences, including the controversial Section 66A, which penalizes sending “*offensive messages*”. Section 66A was later ruled to violate the fundamental right to freedom of speech and expression, as was struck down in the case of *Shreya Singhal v Union of India*¹³⁴. However, when we analyze the Act in the context of data protection laws, it reveals substantial limitations and gaps.

2.3.4 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011¹³⁵. While the IT Act of 2000 primarily focused on cybercrimes and e-commerce, the IT Rules 2011 marked a significant step towards safeguarding **sensitive personal data** (SPD). Rule 3 defines “*sensitive personal data*” such as financial records, health data, sexual orientation, biometric information, etc., and mandates that organizations must obtain “*explicit consent*”¹³⁶ from individuals before collecting or sharing such information¹³⁷. Entities are also required to implement “*reasonable security practices*” (Rule 8), like encryption, access controls. Importantly, users must be informed about data use, retention, and rights. and laid the foundation for the evolution of more comprehensive data protection laws in India.

¹³⁴ *Shreya Singhal v Union of India*- AIR 2015 S.C 1523

¹³⁵ *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*, G.S.R. 313(E), Gazette of India, Apr. 11, 2011, [https://www.meity.gov.in/sites/upload_files/dit/files/GSR313E_10511\(1\).pdf](https://www.meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf).

¹³⁶ The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 5- Collection of information- (1) 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.

¹³⁷ The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 6- Disclosure of Information (1) Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the providers 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.

1. Introduction of the Sensitive Personal Data (SPD) Concept
2. Consent-Based Data Collection and Processing
3. Reasonable Security Practices and Procedures
4. Privacy Policies
5. Grievance Redressal Mechanism

Together, these rules place privacy, transparency, and accountability at the heart of India's digital data ecosystem. The IT Rules 2011 laid the groundwork for more comprehensive data protection laws to follow. The Justice B.N. Srikrishna Committee Report (2018), which played a crucial role in drafting the Personal Data Protection Bill (2019) and, later, the Digital Personal Data Protection Act 2023, inspired the principles embedded in the IT Rules 2011. The IT Rules 2011 were a key stepping stone in India's journey toward a robust data protection regime. While they were limited in scope and faced challenges in implementation, their introduction marked the first time India formally addressed the protection of sensitive personal data in the digital world.

2.3.5 The Information Technology (Intermediaries Guidelines) Rules, 2011 and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rule 2021

The Information Technology (Intermediaries Guidelines) Rules, 2011¹³⁸, framed under Section 79 of the IT Act 2000, govern the responsibilities of intermediaries, such as social media platforms, ISPs, and hosting service providers, concerning the data they handle. In the context of data privacy, these rules mandate that intermediaries observe due diligence while discharging their duties. These Rules attempt to address privacy concerns by discouraging the misuse of personal data and sensitive information by implementing all reasonable measures to secure their computer systems and the information stored within them as per the provisions of the Information Technology (Reasonable Security Practices and Procedures and Sensitive

¹³⁸ *The Information Technology (Intermediaries Guidelines) Rules, 2011*, G.S.R. 314 (E), Gazette of India, Apr. 11, 2011, https://www.meity.gov.in/writereaddata/files/GSR314E_10511%281%29_0.pdf.

Personal Data or Information) Rules, 2011¹³⁹. Rule 3 specifies that intermediaries must publish terms and conditions requiring users not to upload or share any content that is obscene, defamatory, or invasive of privacy. Additionally, for effective incident management, Rule 9 emphasizes reporting cybersecurity incidents by the intermediaries to the Indian Computer Emergency Response Team (CERT-In). Overall, while the rules set some foundational measures for intermediary accountability, they fall short of addressing the broader and nuanced aspects of data privacy.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rule 2021¹⁴⁰ reflects a policy evolution aimed at safeguarding data privacy and users' autonomy in the digital ecosystem. Under Rule 3(1)(a), intermediaries are required to publish a clear privacy policy and user agreements, accessible in multiple Indian languages. Rule 3(1)(b) mandates proactive communication of these policies to users. This requires digital platforms to inform users clearly and in their preferred languages about content restrictions and privacy policies. Users must not post or share anything that violates privacy, promotes harm, impersonates others, infringes rights, or spreads false or offensive information. This includes banning unverified online games and their ads. This goal is to foster a safer digital space by holding users and platforms accountable for harmful, illegal or misleading content. Rule 3 (1)(i) binds intermediaries to comply with the IT Rule 2011, enforcing reasonable security practices such as encryption. Rule 3(1)(h) prescribes a 180-day retention period for users' data post-deactivation. Rule 3(1)(m)¹⁴¹ introduces a normative shift by embedding privacy and transparency as operational duties. Together, these provisions assert user-centric digital governance and prioritize accountability in data handling.

¹³⁹ The Information Technology (Intermediaries Guidelines) Rules, 2011, Rule number 8.

¹⁴⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rule 2021, GSR 139 (E), Gazette of India, Feb. 25, 2021, <https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf>.

¹⁴¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rule 2021, Rule 3(1)(m) the intermediary shall take all reasonable measures to ensure accessibility of its services to users along with reasonable expectation of due diligence, privacy and transparency.

2.3.6 Aadhaar and the Rise of Digital Identity

In 2009, the Indian government launched the Aadhaar project¹⁴², a biometric-based digital identity program, which required the collection of personal data from millions of Indian citizens. This raised concerns about the potential for misuse of personal data and the absence of robust legal safeguards to protect it. The debate around Aadhaar escalated when the government sought to make Aadhaar mandatory for accessing various services. *The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Aadhaar Act)*,¹⁴³ as amended, it represents a pivotal legislative framework governing the collection and usage of biometric and demographic data in India. Within the broader landscape of Indian data protection laws, the Act intersects significantly with principles of informational privacy and personal data governance. Notably, the Act authorized the Unique Authority of India (UIDAI) to collect and manage personal data to authenticate identity for welfare distribution, yet several provisions raise critical concerns under the evolving jurisprudence of data protection post *Justice K.S. Puttaswamy v Union of India* (2017),¹⁴⁴ which affirms the right to privacy as a fundamental right under Article 21 of the Indian Constitution. The Aadhaar Act impose certain safeguards, such as limiting data sharing and enabling user consent for authentication, yet its architecture lacks several core principles outlined in comprehensive data protection regimes, such as purpose limitations, data minimization, and independent oversight. While the 2019 amendments¹⁴⁵ introduce stricter control and limit the scope of private sector use, the Act remains criticized for potential surveillance and inadequate transparency.

Section 29¹⁴⁶ explicitly prohibits the sharing of core biometric information, including fingerprints and iris scans, for any reason other than Aadhaar authentication.

¹⁴² *A Unique Identity for the people Aadhaar: An Overview*, Unique Identification Authority of India, Govt. of India, https://www.uidai.gov.in/images/Aadhaar_Brochure_July_22.pdf.

¹⁴³ The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016, (No. 18), Act of Parliament, Mar. 25, 2016 (India).

¹⁴⁴ Justice K S Puttaswamy (Retd), and Anr vs. Union of India and Ors- (2017) 10 SCR 569.

¹⁴⁵ *The Aadhar and Other Laws (Amendment) Act 2019*, (No. 14), Act of Parliament, 2019 (India).

¹⁴⁶ The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, (No 18) § 29 Restriction on sharing information –(1) 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 the generation of Aadhaar number and authentication under this Act.

This biometric data cannot be disclosed, published, or displayed, even with consent. Under Section 28¹⁴⁷, the Unique Identification Authority of India (UIDAI), as the custodian of Aadhaar data, is entrusted with the security and confidentiality of identity information. This includes the obligation to adopt robust security practices, prevent unauthorized access, and ensure the protection of personal data from breaches or misuse. Section 30¹⁴⁸ of the Act elevates biometric data to the legal status of “*sensitive personal information*”¹⁴⁹, thereby acknowledging its heightened risk in digital identity systems. This classification aligns Aadhaar’s data protection regime with broader privacy norms under Indian law and global best practices. Furthermore, section 37 criminalizes the intentional disclosure, transmission or dissemination of identity information without authorization. Violators face penalties, including imprisonment of up to three years, or a fine of rupees ten thousand (₹ 10,000/-) and which may extend to rupees one lakh (₹ 1,00,000/-) for a company, which underscores the seriousness of unlawful data exposure.

2.3.7 The Judicial Push: Recognition of Privacy as a Fundamental Right (from 2017 to 2023)

1. Justice K. S. Puttaswamy (Retd) & Anr. v. Union of India & Ors¹⁵⁰(2018)- The landmark judgement *Justice K. S. Puttaswamy (Retd) & Anr. Vs. Union of India & Ors* marked a transformative moment in Indian constitutional law by recognizing the right to privacy as a fundamental right under the Constitution. Delivered by a unanimous nine-judge bench of the Supreme Court, the ruling held that privacy is

¹⁴⁷ The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, (No 18) § 28 Security and confidentiality of information- (1) The Authority shall ensure the security of identity information and authentication records of individuals. (2) Subject to the provisions of this Act, the Authority shall ensure confidentiality of identity information and authentication records of individuals. (3) 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 damages.

¹⁴⁸ The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, (No 18) § 30 Biometric information deemed to be sensitive personal information- 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 information”.

¹⁴⁹ 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 (Act no 21 of 2000).

¹⁵⁰ Justice K. S. Puttaswamy (Retd) & Anr. Vs. Union of India & Ors- (2018) 8 SCR 1.

intrinsic to the right to life and personal liberty under Article 21 of the Indian Constitution and is also intertwined with other rights enriched in part III, including Articles 14, 19 and 25. The Court overruled the earlier decisions in *M.P. Sharma and Others vs Satish Chandra*¹⁵¹ (1954) and *Kharak Singh v State of UP and Ors*¹⁵² (1964), which denied the existence of a constitutionally protected right to privacy. Crucially, the judgment conceptualized privacy as encompassing bodily integrity, personal autonomy, decisional freedom, and informational self-determination. In the context of an increasingly data-driven society, the Court underscored the significance of informational privacy and the need to safeguard individuals against arbitrary surveillance by the state and misuse of personal data by private actors. It articulated a threefold test: **legality, necessity and proportionality**¹⁵³ to evaluate any state action infringing upon privacy. This ruling laid the normative foundation for future data protection frameworks in India and aligned the country with international privacy standards.

2. *Navtej Singh Johar & Ors. v. Union of India Thr. Secretary, Ministry of Law and Justice*¹⁵⁴ - The *Navtej Singh Johar & Ors. Vs. Union of India* judgment marks a watershed moment in Indian constitutional jurisprudence, especially in contextualizing the Right to Privacy as a foundational element of dignity, autonomy, and identity. The Supreme Court, while decriminalizing consensual same-sex relations under Section 377 of the Indian Penal Code, rooted its reasoning in the constitutional recognition of privacy as affirmed in *Justice K S Puttaswamy v Union of India* (2017). The Court emphasized that privacy is not merely the “**right to be alone**” but includes the autonomy of individuals in making intimate personal choices, including sexual orientation. The plurality of opinions in the judgment unified around the principle that state interference in consensual adult relationships violates Articles

¹⁵¹ *M.P. Sharma and Others vs Satish Chandra*- 1954 AIR 300, 1954 SCR 1077.

¹⁵² *Kharak Singh v State of UP and Ors* – (1964) 1 SCR 332.

¹⁵³ *Justice K. S. Puttaswamy (Retd) & Anr. Vs. Union of India & Ors*- (2018) 8 SCR 1- (para 417)- the court also laid down the triple test which needs to be satisfy for judging the permissible limits for invasion of privacy while testing the validity of any legislation. These are: (a) The existence of a law. (b) A “legitimate State interest”, and (c) Such law should pass the “test of proportionality”.

¹⁵⁴ *Navtej Singh Johar & Ors. Vs. Union of India Thr. Secretary Ministry of Law and Justice*- (2018) 7 SCR 379.

14, 15, 19, and 21 of the Constitution. Particularly, the right to privacy was interpreted to safeguard the inner sanctum of personal life, insulating individuals from intrusive state action rooted in Victorian morality. The judgment not only invalidated a colonial legal relic but also showed a shift towards substantive equality and a liberal democratic vision of constitutional morality. It has since served as a cornerstone for LGBTQ+ rights and has reoriented the trajectory of privacy jurisprudence in India.

3. *Joseph Shine v. Union of India*¹⁵⁵ (2018)- The judgment marks a transformative moment in Indian constitutional jurisprudence, particularly in reinforcing the Right to Privacy. The Supreme Court unanimously struck down section 497 of the Indian Penal Code, which criminalizes adultery, as unconstitutional. Central to the Court's reasoning was the inviolability of individual autonomy and dignity under Article 21 of the Constitution, which the Court had earlier affirmed in *Justice K S Puttaswamy (Retd.) v Union of India* (2017). The judgment held that criminalizing consensual sexual relationships among adults, even if outside marriage, intrudes into the private sphere of individual life, a domain protected under the right to privacy. The court emphasized that the provision was manifestly arbitrary and patriarchal and violated women's autonomy by treating them as property. It underscored that morality cannot trump constitutionally guaranteed rights, and the law must evolve with social and constitutional morality rather than static societal norms. The decisions thus not only decriminalized adultery but also fortified the privacy jurisprudence in India, showing a shift towards greater recognition of personal liberty, equality, and individual choice within intimate relationships.

4. *Dr. Sabu Mathew George v. Union of India & Others*¹⁵⁶ (2018)- This case focused on a critical intersection between technology, public health and constitutional privacy rights. The petitioner, a public health activist, raised concern over the unrestricted availability of online advertisements and search results related to sex selective abortions, which contravened the Pre-Conception and Pre-Natal Diagnostic

¹⁵⁵ *Joseph Shine v Union of India* (2018) 11 SCR 765.

¹⁵⁶ *Dr. Sabu Mathew George v Union of India & Others* – AIR 2018 SC 578.

Techniques (Prohibition of Sex Selection) Act 1994¹⁵⁷. The Supreme Court examined the responsibility of search engines in regulating content that could potentially facilitate female feticides, a persistent social issue in India. It contributes to the evolving jurisprudence post *K S Puttaswamy v Union of India* (2017) by highlighting how algorithmic governance, private tech and state regulation must navigate the terrain of the digital ecosystem and ethical use of Artificial Intelligence.

5. *Anuradha Bhasin v Union of India & Ors*¹⁵⁸ (2020)- The Supreme Court decision in *Anuradha Bhasin v Union of India* (2020) marks a landmark judicial clarification on the Constitutional parameters surrounding internet shutdown and restrictions under Section 144 of the CrPC. The court emphasized that indefinite suspension of internet service is impermissible and must adhere to the principle of proportionality and necessity. It recognizes the internet as a vital medium for trade and freedom of expression, thereby affirming that such rights are protected under Article 19(1)(a) and 19(1)(g) of the Indian Constitution. Additionally, the judgment underscores the need for publication of government orders, judicial review of restrictions, and time-bound reviews of telecom suspension, establishing transparency and accountability as integral to democratic governance.

2.4 REPORTS OF VARIOUS COMMITTEES

2.4.1 Justice Ajit Prakash Shah Committee (2011)

The first comprehensive move toward data protection came with the Justice A.P. Shah Committee report in 2012¹⁵⁹, which advocated for a privacy framework grounded in key principles like notice, consent, purpose limitation, and accountability. This report highlighted the importance of protecting personal data and served as a precursor to later legislative efforts. Report of the Group of Experts on Privacy, chaired by Justice

¹⁵⁷ Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act 1994, (No. 57) Act of Parliament, 1994 (India).

¹⁵⁸ *Anuradha Bhasin v Union of India & Ors* (2020) 1 SCR 812.

¹⁵⁹ Report of the Group of Experts on Privacy, Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court, dated 16th October 2012, <https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf> (Last visited Dec. 23, 2024).

A. P Shah, is a landmark document that lays a foundational framework for privacy rights and data protection in India. The report expresses concern about the rapid and unregulated collection of personal data by both government and private actors. It underscores the inadequacy of existing legal frameworks and emphasizing the need for a comprehensive Privacy Act. The committee released its report in 2012 and recommended the creation of an overarching law for privacy protection based on five salient features:

- (i) Technological neutrality and interoperability with international standards,
- (ii) Multi-dimensional privacy,
- (iii) Horizontal applicability,
- (iv) Conformity with privacy principles, and
- (v) Co-regulatory enforcement regime.

The report also featured nine national privacy principles central to the interpretation of the right to privacy. These national privacy principles were intended to establish safeguards and procedures for the processing of data, as well as establish the rights of the people in relation to their data. A co-regulatory enforcement model is recommended, involving both Privacy Commissioners and sectoral Self-Regulatory Organizations (SROs), to ensure compliance while maintaining adaptability to sector-specific needs. The report also highlights the horizontal application of privacy law to both state and non-state actors. The report presents a nuanced, inclusive, and forward-looking vision for privacy governance in India¹⁶⁰.

2.4.2 Justice B.N. Srikrishna Committee (2018)

The Committee Report on the Draft Data Protection Bill, 2018, chaired by Justice B.N. Krishna¹⁶¹, represents a seminal effort to conceptualize a data protection framework tailored to India's democratic ethos and digital aspirations. Against the

¹⁶⁰ Report of the Group of Experts on Privacy, Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court, dated 16th October 2012, <https://cis-india.org/internet-governance/blog/report-of-group-of-experts-on-privacy.pdf> (Last visited Dec. 23, 2024).

¹⁶¹ *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, July 27, 2018, https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf (Last visited Dec. 23, 2024).

backdrop of increasing digitalization and the Supreme Court's affirmation of privacy as a fundamental right in *Puttaswamy v Union of India*, the report provides a balance between individuals' autonomy with the growth potential of a data-driven economy. Framing its recommendation as a “Fourth Way” to create a privacy regime rooted in empowerment, fairness and digital trust. The report is the recognition of citizens as “data principals” and data processors as “data fiduciaries”, emphasizing the fiduciary obligation to process data transparently, fairly, and within the bounds of consent. The report also identifies critical data rights, including access, correction, portability, and the right to be forgotten and proposes obligations such as purpose limitation, storage minimization and breach notification. It acknowledges sector-specific challenges and proposes an agile regulatory body, the Data Protection Authority (DPA), to enforce compliance through guidance, codes of practice and penalties.

2.5 DATA PROTECTION BILLS

The proposed data protection bills were designed to safeguard individual privacy concerning personal data by establishing comprehensive standards for the collection, processing and transfer of the data. The framework outlines mechanisms to ensure transparency, accountability, and fairness in data processing practices.

2.5.1 Personal Data Protection Bill, 2019

The Personal Data Protection Bill 2019¹⁶² represents a pivotal legislative initiative aimed at institutionalizing data privacy as a fundamental right in India. Framed in the context of rapid digitalization and landmark judicial recognition of privacy. The bill establishes a comprehensive legal infrastructure for the processing, protection, and governance of personal data. The key feature of the bill is the establishment of the Data Protection Authority of India, endowed with the power to monitor compliance. Significantly, the bill’s balanced approach to data protection with innovation. The bill articulates a rights-oriented yet pragmatic approach to data governance. The bill outlines the core principles of data processing, including purpose limitation, data minimization, notice, and consent, and introduces individual rights such as data

¹⁶² The Personal Data Protection Bill 2019, Bill no 373 of 2019, (India).

access, correction, portability, and the right to be forgotten. It also regulates the processing of sensitive personal data and children's data with heightened safeguards.

2.5.2 Data Protection Bill 2021

The Joint Committee on the Personal Data Bill 2019¹⁶³ presents a comprehensive legislative effort by the Indian Parliament to establish a legal framework for the protection and governance of personal data. The report finalized on 16th December 2021 addresses the growing concern over the ethical use, security, and sovereignty of digital data in an increasingly interconnected world. It responds to the Supreme Court of India's landmark recognition of privacy as a fundamental right, which catalyzed the need for a robust data protection regime. Anchored in principles of transparency, accountability, and individual autonomy, the Committee's report recommends a nuanced regulatory mechanism that balances innovation and privacy, proposing the establishment of a Data Protection Authority to oversee compliance. The key recommendations reflect a deep engagement with global best practices, including elements from the EU General Data Protection Regulation, while adapting them to India's socio-political context. The Committee suggests expanding the Bill's scope to include both personal and non-personal data¹⁶⁴ under a unified law, enhancing the government's role in data governance. It underscores the necessity of explicit user consent, data localization¹⁶⁵, and safeguards against profiling and surveillance, while allowing for specific exemptions in the interest of national security and public order. Additionally, the report offers clarity on the obligations in the interest of national security and public order. Additionally, the report offers clarity on the obligations of data fiduciaries and processors, children's data, and cross-border data flows.

¹⁶³ The Report of the Joint Committee on the Personal Data Protection Bill, 2019, JCPDPB 2019, Seventh Lok Sabha, Lok Sabha Secretariat, Dec. 16, 2021, and laid in Rajya Sabha on Dec.16, 2021, https://prsindia.org/files/bills_acts/bills_parliament/2019/Joint_Committee_on_the_Personal_Data_Protection_Bill_2019.pdf (Last visited Dec. 23, 2024).

¹⁶⁴ The Personal Data Protection Bill 2021, §. 2 Application of the Act to processing of Personal and non-personal data.

¹⁶⁵ The Personal Data Protection Bill 2021, § 33- Prohibition on processing of sensitive personal data and critical personal data outside India. (1) Subject to the conditions provided 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. (2) The critical personal data shall only be processed in India.

Critically, the Committee recommends renaming the Bill to the “*Data Protection Bill 2021*” to reflect a broader legislative intent. By proposing a more inclusive and comprehensive data framework, the Committee emphasizes India’s ambition to assert digital sovereignty and foster a rights-based data economy. While the report strengthens institutional mechanisms, it also highlights tension between individual rights and state interest, inviting further academic and policy discourse on balancing privacy with governance imperatives in the digital age.

2.5.3 The Digital Personal Data Protection Bill, 2022

In 2017, the Central government established a Committee of Experts on Data Protection under the leadership of Justice B.N. Srikrishna to explore key issues surrounding personal data governance in India. The Committee presents its findings in July 2018, laying the groundwork for legislative action. Acting on its recommendations, the government introduced the Personal Data Protection Bill in the Lok Sabha in December 2019. This Bill was subsequently referred to the Joint Parliamentary Committee, which submitted its review and recommendation in December 2021. However, in August 2022, the government decided to withdraw the Bill from Parliament. Following this, in November 2022, the Ministry of Electronics and Information Technology published a draft of the Digital Personal Data Protection Bill 2022 for public consultation¹⁶⁶. The Digital Personal Data Protection Bill 2022, introduced by the Government of India, represents a landmark initiative toward establishing a comprehensive legal framework for the protection and governance of personal data in the digital age. It delineated the responsibilities of data fiduciaries and rights of data principals, drawing from global standards. Bill emphasizes storage limitation and data minimization ensuring that data is collected only for lawful, specific purposes and processed in a manner that is necessary and proportionate. The bill classifies entities as “*data fiduciary*” and “*data processors*”, and assigns specific duties to each while endowing data principals with clearly defined rights. It introduced

¹⁶⁶ Draft Digital Personal Data Protection Bill 2022, Ministry: Electronics and Information Technology, PRS India, <https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022> (last visited Dec. 25, 2024).

the provisions of “*deemed consent*”¹⁶⁷ in scenarios involving public interest and emergencies, introducing ambiguities and potential for overreach, particularly when it comes to the State’s broad exemptions.

2.5.4 The Digital Personal Data Protection Bill 2023

The Digital Personal Data Protection Bill 2023¹⁶⁸, as introduced in the Indian legislative landscape, establishes a comprehensive framework that balances the protection of individual privacy with the facilitation of lawful data processing. The bill underscores the significance of digital personal data, defined as information that can identify an individual, and articulates both obligations of Data Fiduciaries (such as companies, individuals, or government bodies handling such data) and the rights and duties of Data Principals. It envisions a legal structure that not only upholds individuals' rights but also imposes financial penalties for non-compliance, thus reinforcing accountability in digital interactions. The bill aims to modernize India’s data protection environment with minimal disruption to current operations, while also enhancing citizen convenience and improving business competitiveness. Rooted in seven core principles¹⁶⁹

1. The principle of consented, lawful and transparent use of personal data.
2. The principle of purpose limitation.
3. The principle of data minimization.
4. The principle of data accuracy.
5. The principle of storage limitation.
6. The principle of reasonable security safeguards and
7. The principle of accountability.

¹⁶⁷ Deemed consent- A Data Principal is deemed to have given consent to the processing of her personal data if such processing is necessary: (1) in a situation where the Data Principal voluntarily provides her personal data to the Data Fiduciary and it is reasonably expected that she would provide such personal data.

¹⁶⁸ The Digital Personal Data Protection Bill 2023, Bill no 113 of 2023, <https://sansad.in/ls/legislation/bills> (last visited Dec. 25, 2024).

¹⁶⁹ Salient Feature of the Digital Personal Data Protection Bill 2023, Ministry of Electronics and IT, 9th August 2023, PIB, New Delhi, <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264> (Last visited Dec. 25, 2024).

Notably, the bill adopts inclusive language by using “*she*” instead of the traditional “*he*”. The bill guarantees key rights such as access to personal data, correction and erasure of inaccuracies, redressal of grievances, and the ability to nominate someone to exercise data rights. On the fiduciary side, the bill imposes critical responsibilities including maintaining robust security measures, timely reporting of data breaches, erasing data upon consent withdrawal and offering grievance redressal systems. Further, the bill protects children’s data, mandating parental consent for processing and strictly prohibiting practices that could harm children’s well-being, such as behavioural tracking or targeted advertisement. Collectively, the bill reflects India’s attempt to craft a simplified yet principled data protection regime that respects individual autonomy while supporting the growth of its digital economy. As per the bill entrusted, the Data Protection Board is entrusted with responsibilities and empowered to issue directives aimed at mitigating data breaches and to conduct inquiries into such incidents, including complaints lodged by data principals. The Board may impose penalties on errant data fiduciaries. In case of repeated non-compliances, the Board can recommend that the government block access to the offending entity’s platform, such as a website or app.

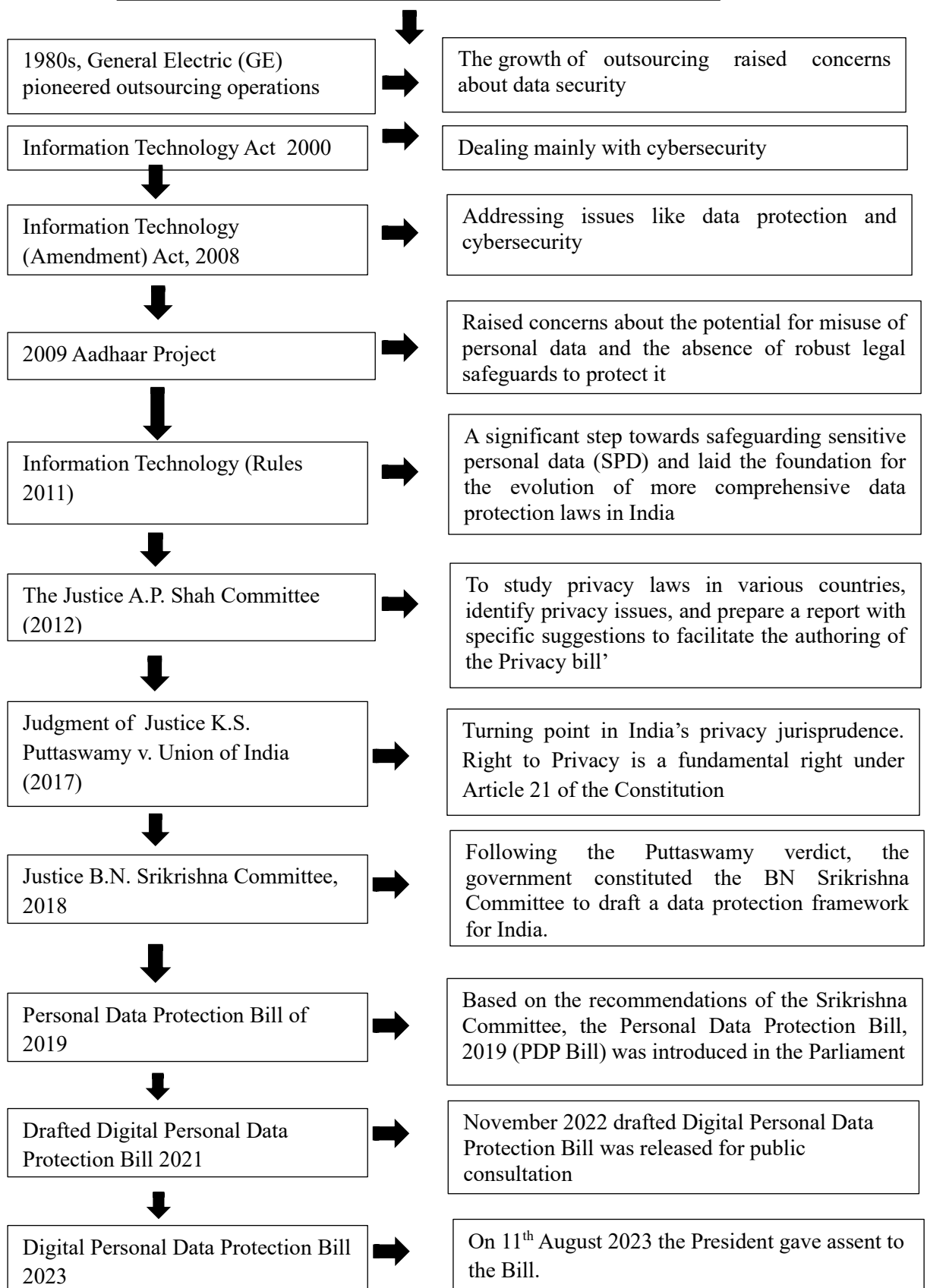
2.5.5 Comparative Analysis Data Protection Bills: A Snapshot

After several years of deliberation and four successive versions, India has finally enacted a formal data protection law. The journey from conceptualization to legislation has been marked by substantial evolution. A comparative analysis is illustrated in Table 2.1 evaluates the key dimensions of the transformative nature of the legislative process.

The Draft Personal Data Protection Bill, 2018	The Personal Data Protection Bill, 2019	Recommendation of the Joint Parliamentary Committee	The Draft Digital Personal Data Protection Bill 2023
Scope and Applicability			
Processing of Personal Data i) Within India ii) Outside India	Expands the scope under the 2018 bill to include anonymized personal data	Processing of Personal and Non-Personal Data	As compared to the 2018 bill, it removes the reference to business carried out in India, and also does not cover offline personal data and non-automated processing
Reporting of Data Breaches			
Fiduciary to notify the Data Protection Authority about a data breach, and the Authority will decide whether to notify the data principal or not	Same as the 2018 Bill	All breaches, regardless of potential harm, must be reported to the Authority within 72 hours	Every personal data breach must be reported to the Data Protection Board of India and each affected data principal.
Right to Data Portability and Right to be Forgotten			
Both rights were provided	Both rights were provided	Both rights were provided	Not provided
Transfer of Personal Data outside India			
i) Every fiduciary is required to store at least one serving copy of personal data in India	i) A copy of sensitive personal data should remain in India.	Sensitive personal data will not be shared with foreign agencies without prior approval from the central government	i) No classification of sensitive and critical personal data.
ii) May be transferred outside India, if consent is provided, to certain permitted countries or under a contract approved by the Authority	ii) Certain sensitive personal data may be transferred only if explicit consent is provided, with no restriction on other personal data.		ii) Personal data can be transferred if notified by the central government, subject to the prescribed terms and conditions.
iii) Certain critical data can be processed only in India.	iii) On critical personal data, the same as the 2018 Bill		
Table 2.1: Key differences between various drafted Data Protection Bills¹⁷⁰			

¹⁷⁰ <https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022> (Last visited Dec. 25, 2024).

Figure 2.1: Timeline of Indian Data Protection Laws



2.6 DIGITAL PERSONAL DATA PROTECTION ACT 2023

India's Digital Personal Data Protection Act 2023¹⁷¹ (hereinafter referred to as DPDP Act) reached a significant milestone after years of deliberation, revision, and public discourse. It was officially passed by the Indian Parliament and received the assent of the President on August 11, 2023, marking the culmination of a long legislative journey. However, while the Act has been enacted, the official date for its implementation is yet to be declared. The Act marks a seminal moment in India's journey towards formalizing a structured legal framework for personal data governance in the digital age. Enacted with the dual aim of empowering individuals over their personal data while facilitating legitimate processing by state and private actors. The Act embodies a consent-centric approach with ancillary grounds for non-consensual processing under defined conditions. The Digital Personal Data Protection Act 2023 is specifically concerned with digital personal data, excluding non-personal data from its scope. Upon its formal implementation, the Act is set to suspend section 43A of the Information Technology Act 2000 along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rule 2011¹⁷².

2.6.1 Key Concepts and Definitions under the Act

At the heart of this framework lie key definitions and concepts that determine the scope of rights, responsibilities, and regulatory oversight. Understanding these terms is critical for interpreting how the Act functions in practice. These definitions lay the foundational vocabulary of India's emerging data protection regime.

1. Personal Data- *“Any data about an individual who is identifiable by or in relation to such data”*.¹⁷³ This broad definition ensures that any information, whether direct (like name, phone number), falls under the ambit of the Act if it can be linked to a specific person. The emphasis is on identifiability rather than the type or format of data.

¹⁷¹ The Digital Personal Data Protection Act 2023, (No. 22), Act of Parliament, 2023, (India).

¹⁷² The Digital Personal Data Protection Act, 2023, § 44 (India).

¹⁷³ The Digital Personal Data Protection Act 2023, § 2(t) (India).

2. Data Principal- “*Data Principal*”¹⁷⁴ in simple terms, the data Principal is the data subject, the person whose data is being collected, stored, processed or shared. The DPDP Act grants this individual several rights, thereby shifting power toward the user.

3. Data Fiduciary- “*Data Fiduciary*”¹⁷⁵ any person, company, firm, government body, or organization that determines the purpose and means of processing personal data (the entity processing the data). This term aligns with the concept of a data controller in global data protection laws. The Data Fiduciary is the primary decision-maker about how and why personal data is handled. It bears the responsibility of ensuring lawful processing, securing data and enabling user rights.

4. Data Processor- “*means any person who processes personal data on behalf of a Data Fiduciary*”¹⁷⁶. This actor doesn’t decide what to do with data but executes the instructions of the Data Fiduciary. For example, outsourced IT service providers, cloud platforms, or analytics firms. While they are bound by the Act, the Fiduciary remains primarily accountable.

5. Processing- *Processing*¹⁷⁷ means any operation performed on digital personal data. This includes everything from collection, storage, retrieval, transmission, and erasure to profiling and algorithmic decision-making. Importantly, the DPDP Act applies only to digital personal data or data that is digitalized.

6. Consent – Free, specific, informed, unconditional, and unambiguous, indication of the Data Principle’s willingness to allow data processing¹⁷⁸. Consent must be given through a clear affirmative action, and the user must be able to withdraw consent as

¹⁷⁴ The Digital Personal Data Protection Act 2023, § 2(j) “Data Principal” means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means; (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf;

¹⁷⁵ The Digital Personal Data Protection Act 2023, § 2(i) “Data Fiduciary” means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

¹⁷⁶ The Digital Personal Data Protection Act 2023, § 2(k) (India).

¹⁷⁷ The Digital Personal Data Protection Act 2023, § 2(x) processing in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaption, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

¹⁷⁸ The Digital Personal Data Protection Act 2023, § 6(1), and s 7(a) (India).

easily as they gave it. The Act emphasizes purpose limitation; data should only be processed for the purpose for which consent was given.

Notably, the Act does not define ‘*sensitive personal data*’,¹⁷⁹ a major omission given the high stakes around biometric data, health information and financial records and non-inclusion of ‘*non-personal data*’¹⁸⁰ within the ambit of the DPDP Act 2023. Similarly, there is no distinction between *volunteered*, *observed*, and *inferred* data, a critical gap as AI systems increasingly rely on inferred profiles to make decisions about individuals. Unlike the European Union’s DGPR, India’s DPDP Act does not refer to non-personal data or anonymized datasets, even though much of India’s digital public infrastructure (e.g., Cowin, Digi Locker, ONDC) depends on anonymized data flows. This omission creates a regulatory vacuum for AI training, algorithmic bias and predictive analytics, which are often powered by such datasets.

2.6.2 The Key Features of the Act

The Digital Personal Data Protection Act 2023 is a dedicated legislation aimed at protecting individuals' personal data. It defines personal data as any information linked to an identifiable person, whether directly or indirectly. The Act introduces key terms such as consent, data principal, data fiduciary, and significant data fiduciary. The key features of the Act are:

i. Scope of the Act: The Digital Personal Data Protection Act 2023 defines digital personal data as information collected in digital form or digitalized post-collection¹⁸¹. The Act aims to regulate the processing of such data by both public and private entities, ensuring lawful, transparent, and accountable data handling practices across sectors. The Act also applies to the processing of personal data conducted outside

¹⁷⁹ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), r. 3 (India).

¹⁸⁰ MeITY Reports by the Committee of Experts on Non-Personal Data Governance Framework defines Non-Personal Data into three categories: (1) Public Non-Personal Data, (2) Community Non-Personal Data and (3) Private Non-Personal Data, <https://psa.run/wp-content/uploads/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf>.

¹⁸¹ Digital Personal Data Protection Act 2023, § 3. Subject to the provisions of this Act, it shall— (a) apply to the processing of digital personal data within the territory of India where the personal data is collected— (i) in digital form; or (ii) in non-digital form and digitised subsequently.

India, provided it relates to offering goods or services to individuals located within the Country.

ii. Consent Framework: The Act emphasizes consent-based data processing as outlined in sections 6¹⁸² and 4¹⁸³, personal data can only be processed with the free, informed, specific and unambiguous consent of the Data Principal.

iii. Regulatory Oversight and Enforcement Mechanisms: Sections 18-22 establish the Data Protection Board of India as the principal regulatory and adjudicatory body. It is vested with the powers to investigate data breaches, mediate disputes, issue binding directions, and impose financial penalties, which may extend up to ₹ 250 crore depending on the severity of the breach (Schedule I).

iv. Exemptions and Government Powers: While DPDPA sets a robust compliance framework, section 17 provides broad exemptions for government and notified entities, ostensibly for national security, law enforcement, or public order purposes. Critics argue that such wide discretionary powers could weaken checks on state surveillance.

v. Cross-Border Data Transfer: Section 16 of the Act permits cross-border data transfer to countries notified by the central government. This approach aligns with international trade norms while allowing strategic oversight.

2.6.3 Principles of Data Privacy

i. Consent-Based Processing of Data: Consent forms the very foundation of the DPPD Act. It ensures that individuals, known as data principals, have the power to decide how their personal data is used. Under this principle, data can only be processed after obtaining the individual's free, informed, specific and unambiguous

¹⁸² Digital Personal Data Protection Act 2023 (No 22) § 6 (1) The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.

¹⁸³ Digital Personal Data Protection Act 2023 (No 22) §4 (1) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose- (a) for which the Data Principal has given her consent.

consent. The consent must be requested in plain and understandable language, preventing misuse or confusion. Data principals also have the right to withdraw their consent at any time, and once withdrawn, processing must stop immediately.

ii. Purpose Limitation: It ensures that personal data is collected only for a specific, lawful, and clearly stated purpose. Once that purpose is fulfilled, the data cannot be reused for unrelated or secondary objectives without obtaining fresh consent from the individual.

iii. Data Minimization: Data minimization is based on the idea that organizations should collect only the minimum amount of personal data necessary for achieving the intended purpose.

iv. Accuracy of Personal Data: Accuracy is vital for ensuring fairness and reliability in data processing. The DPDP Act requires data fiduciaries to ensure that the personal data they store or use is complete, accurate, and up-to-date.

v. Storage Limitation: The personal data must not be stored longer than necessary to fulfil the specific purpose for which it was collected. Once the objective is achieved, the data must be deleted to prevent misuse. This encourages data fiduciaries to establish data retention policies.

vi. Protection for Children's Data: The DPDP Act provides special protection for individuals below 18 years of age. Processing of a child's personal data requires verifiable parental consent, ensuring that minors are not exploited.

vii. Penalties and Enforcement: The enforcement mechanism under the DPDP Act is robust and deterrent in nature. Penalties can be imposed up to ₹ 250 crore for offences. This strict penalty regime promotes corporate accountability and compliance.

2.6.4 Rights and Obligations under the Digital Personal Data Protection Act 2023

The Digital Personal Data Protection Act 2023 marks a transformative shift in India's approach to regulating the digital ecosystem. Rooted in the principles of consent, purpose limitation, transparency, and accountability, the Act establishes a robust framework for rights for individuals referred to as Data Principals and obligations for entities that process their data, known as Data Fiduciaries.

1. Rights of The Data Principal (Section 11-14)

The DPDP Act empowers individuals with a suite of enforceable rights that place them at the centre of data governance. These rights go beyond passive protection and enable active participation in how personal data is handled.

i. Right to Access Information about Personal Data (Section 11): Data Principal has the right to know what personal data is being collected about them, how it is being processed and for what purposes. This includes access to the identities of the data fiduciaries and information about any data shared with third parties. This right empowers individuals to make informed choices and hold institutions accountable. Section 11 of the DPDP Act 2023 grants individuals the *right to access information* about how their personal data is being used. This means that a person can seek any Data Fiduciary to provide a clear summary of what personal data is being processed, how it's being used, and with whom it has been shared. The Data Fiduciary must also disclose the name of any third party (Processors) who received the data and describe what was shared.¹⁸⁴ However, an important exception to this right is that this right does not apply to data that was shared with lawfully authorized entities for purposes

¹⁸⁴ The Digital Personal Data Protection Act 2023, (No 22) § 11 – Right to access information about personal data (1) The Data Principal shall have the right to obtain from the Data Fiduciary to whom she has previously given consent, including consent as referred to in clause (a) of section 7 (hereinafter referred to as the said Data Fiduciary) for processing of personal data, upon making to it a request in such manner as may be prescribed, - (a) a summary of personal data which is being processed by such Data Fiduciary and the processing activities undertaken by that Data Fiduciary with respect to such personal data; (b) the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared by such Data Fiduciary, along with a description of the personal data so shared; and (c) any other information related to the personal data of such Data Principal and its processing, as may be prescribed.

like crime investigation, cybercrime detection, or legal prosecution, where written requests justify such sharing¹⁸⁵.

ii. Right to Correction and Erasure of Personal Data (Section 12): Individuals can request correction of inaccurate or outdated personal data and can also demand deletion of data no longer necessary for the Original purpose. Section 12 of the DPDP Act 2023 empowers individuals with the right to correct, update, complete or erase their personal data. The fiduciary must take action to correct errors, fill in missing details or update the information. Additionally, individuals can request deletion of their data, and the fiduciary is obligated to erase it unless keeping it is legally required or still necessary for the original purpose. This right gives individuals greater control over their digital identity and helps ensure data remains accurate and relevant.

iii. Right to Grievance Redressal (Section 13): Section 13 of the DPDP Act 2023 gives individuals the right to a grievance redressal system. If a Data Principal believes that a Data Fiduciary or *Consent Manager*¹⁸⁶ has mishandled their personal data or failed to uphold their rights, they can file a complaint directly with that entity. The party responsible is required to respond within a time frame specified by the rules. This process ensures accountability and encourages resolution at the earliest possible level.

iv. Right to nominate (Section 14): Section 14 of the DPDP Act 2023 introduces a progressive and compassionate provision, the right to nominate. It allows a Data Principal to designate another person to act on their behalf in case of death or incapacity. This nominee can then exercise the Data Principal's rights, such as requesting data correction, deletion, or access, ensuring continuity and dignity in data

¹⁸⁵ The Digital Personal Data Protection Act 2023, (No 22) § 11 (2) Nothing contained in clause (b) or clause (c) of sub-section (1) shall apply in respect of the sharing of any personal data by the said Data Fiduciary with any other Data Fiduciary authorized by law to obtain such personal data, where such sharing is pursuant to a request made in writing by such other Data Fiduciary for the purpose of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences.

¹⁸⁶ The Digital Personal Data Protection Act 2023, (No 22) § 2(g) Consent Manager means a person registered with the Board, who act as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platforms;

control. This provision acknowledges that digital rights should not end with a person's life or health limitations and promotes responsible human-centric data ownership.

v. *Right to Withdraw Consent:* Consent under the DPDP Act must be free, informed, specific and unambiguous and just as importantly, it must be revocable. Individuals can withdraw their consent at any time, and the Data Fiduciary is obligated to stop processing their data once consent is withdrawn¹⁸⁷.

2. Obligations of The Data Fiduciary (Data-Handling Entity)

While the DPDP Act empowers individuals, it also imposes corresponding duties on data fiduciaries, ensuring that data is collected and processed in a lawful, fair, and transparent manner.

i. *Obligation to Process Lawfully and Fairly:* Data Fiduciaries must ensure that personal data is collected only with valid consent or under legally permitted grounds. Data must not be processed beyond the stated purpose (i.e. purpose limitation).

ii. *Obligation to Maintain Data Security:* Every Data Fiduciary is required to implement reasonable technical and organizational safeguards to prevent data breaches, unauthorized access, or data loss. The Act obliges them to notify the Data Protection Board in case of a breach¹⁸⁸.

iii. *Obligation to Erase upon purpose Completion:* Data that has fulfilled its intended purpose or is no longer necessary must be deleted. This aligns with the principle of data minimization, helping to avoid the long-term risk of retention and profiling¹⁸⁹.

¹⁸⁷ The Digital Personal Data Protection Act 2023, (No 22) § 6 (6) If a Data Principal withdraws her consent to the processing of personal data under sub-section (5), the Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing the personal data of such Data Principal unless such processing without her consent is required or authorized under the provisions of this Act or the rules made thereunder or any other law for the time being in force in India.

¹⁸⁸ The Digital Personal Data Protection Act 2023, (No 22) § 8(5) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.

¹⁸⁹ The Digital Personal Data Protection Act 2023, (No 22) § 8 (7)(a) A Data Fiduciary shall, unless retention is necessary for compliance with any law for the time being in force- (a) erase personal data, upon the Data Principal withdrawing her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier.

iv. Transparency and Accountability: Data Fiduciaries must publish privacy notices in clear, accessible language, detailing how and why data is being collected¹⁹⁰. The law encourages proactive compliance through documentation, audits, and internal oversight mechanisms.

v. Enhanced Compliance for Significant Data Fiduciaries (SDFs): Entities handling large volumes of personal data or dealing with sensitive groups (such as children) are designated as Significant Data Fiduciaries. They are subject to stricter duties such as¹⁹¹:

- Appointment of Data Protection Officer (DPO)
- Regular Data Protection Impact Assessment (DPIAs)
- Periodic security audits.

vi. Children's Data Protection: Processing of personal data of children (under 18 years) requires verifiable parental consent. The law prohibits data processing that may harm a child's well-being and bans tracking, behaviour profiling, and targeted advertising aimed at children¹⁹².

2.6.5 Data Protection Board of India

The Digital Personal Data Protection Act 2023 introduces a structured and centralized enforcement mechanism to ensure that both individuals and organizations are protected and held accountable in the digital data ecosystem. The institutional framework under the DPDP Act is the Data Protection Board of India. The Board is

¹⁹⁰ The Digital Personal Data Protection Act 2023, (No 22) § 5(1) Every request made to a Data Principal under section 6 for consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal informing her;- (i) the personal data and the purpose for which the same is proposed to be processed; (ii) the manner in which she may exercise her rights under sub-section (4) of section 6 and section 13; and (iii) the manner in which the Data Principal may make a complaint to the Board in such manner as may be prescribed.

¹⁹¹ The Digital Personal Data Protection Act 2023, (No 22) § 10 (2) (India).

¹⁹² The Digital Personal Data Protection Act 2023, (No 22) § 9 Processing of personal data of children. (1) The Data Fiduciaries shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed.

Explanation- For the purpose of this sub-section, the expression "consent of the parent" includes the consent of lawful guardian, wherever applicable. (3) A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.

the Central institution responsible for enforcement, dispute resolution, and compliance oversight. This Board functions much like a quasi-judicial authority, similar to regulators in other sectors like telecom or securities. The DPBI is designed to function independently, and it holds the authority to summon parties, conduct hearings, and issue binding orders, strengthening India's digital rights landscape with an accessible and impartial watchdog. Key functions of the Board:

i. *Handling complaints and grievances:* If an individual feels their data rights have been violated and internal grievance mechanisms have failed, they can approach the Board.

ii. *Adjudicating Breaches:* The board is empowered to investigate and decide on data breaches, misuse, or failure by an organization to meet its data protection obligations.

iii. *Imposing Penalties:* It can impose financial penalties for non-compliance, including significant fines for data breaches, consent violations, and failure to report incidents.

iv. *Ensuring Fairness:* The Board ensures that enforcement is proportional, transparent, and just, taking into account the context and severity of each case.

2.7 DIGITAL PERSONAL DATA PROTECTION RULE 2025

The Draft Digital Personal Data Protection Rules 2025¹⁹³ have been introduced as a vital mechanism to enforce and give effect to the Digital Personal Data Protection Act 2023, reflecting India's strategic vision for building a robust and citizen-centric data protection regime. These rules are crafted with an emphasis on clarity, accessibility, and inclusiveness, aiming to uphold individual rights in the evolving landscape of the digital economy. It attempts to address pressing challenges such as unauthorized commercial exploitation of data, data breaches and emerging digital threats¹⁹⁴. The

¹⁹³ Draft DIGITAL PERSONAL DATA PROTECTION RULES 2025, GSR 02 (E.), Gazette of India, Part II, Sec 3(i), Jan. 03, 2025.

¹⁹⁴ *Draft Digital Personal Data Protection Rules 2025*, Research Unit, Press Information Bureau, Government of India, <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/jan/doc202515481101.pdf>,

Digital Personal Data Protection Rule 2025¹⁹⁵ will come into force in different phases. Rules 1, 2 and 17 to 21 will commence on the day they are published in the official Gazette. Rule 4 will commence one year after publication, while Rules 3, 5 to 16, 22 and 23 will take effect eighteen months after publication. This phase approach ensures that individuals and organizations have enough time to understand and prepare for the new data protection requirements¹⁹⁶. A digital-first Data Protection Board will be formed to address complaints and appeals efficiently. These Digital Personal Data Protection Rules 2025 contain 23 Rules and 7 Schedules. 12 Rules are directly applicable to Data Fiduciaries and mandate their compliance, while the remaining 7 rules specifically concentrate on the formation and functioning of the Data Protection Board, detailing its power, responsibility, and operational mechanisms. Rule 1 is dedicated to the application of the rules to the state and its instrumentalities, ensuring accountability in public sector data handling. The remaining two provisions address broader regulatory aspects, complementing the core framework with essential implementation and compliance guidelines. The Rule has 7 schedules, of which four specifically provide detailed guidance to data Fiduciaries, helping them implement necessary measures to ensure compliance with the Data protection frameworks. The other three Schedules focus on the internal functioning and operational procedures of the Data Protection Board, outlining the institutional mechanisms required for its effective governance and enforcement role¹⁹⁷. The key aspects of the Rule are:

1. Strengthening Consent Protocols: It mandates that data fiduciaries issue a clear, detailed, and accessible notice to data principals before collecting any personal data. The draft Rules further emphasize that the language used should be plain, structured, and easily comprehensible.

2. Mandating Robust Security Measures: These include encryption, obfuscation, data masking and role-based access control.

¹⁹⁵ DIGITAL PERSONAL DATA PROTECTION RULES 2025, GSR 846 (E.), (India) Nov. 13, 2025, <https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf>.

¹⁹⁶ Id

¹⁹⁷ *Advent of Privacy Era in India, The Digital Personal Data Protection Rules, 2025*, Ernst And Young LLP, <https://www.ey.com/content/dam/ey-unified-site/ey-com/en-in/insights/cybersecurity/documents/2025/01/ey-india-dpdp-rules-2025-v1.pdf>.

3. Mandatory Breach Notification: The draft Rules clarify that such notifications must be concise, timely, and informative, detailing the nature, extent, timing, impact and remedial actions. The Rules stipulated that the Data Protection Board must be notified within 72 hours of a breach.

5. Consent Manager: As outlined in the Digital Personal Data Protection Act 2023, a Consent Manager is registered with the Data Protection Board that acts as a centralized interface, enabling Data Principals to grant, manage, review and withdraw their consent via a secure and transparent digital platform.

2.8 NAGALAND STATE DATA SHARING AND ACCESSIBILITY POLICY 2024:

The increasing reliance on data-driven decision-making in public administration has underscored the importance of structured and responsible data governance frameworks. In this context, the *Nagaland State Data Sharing and Accessibility Policy 2024*¹⁹⁸ emerges as a landmark initiative, reflecting the state's commitment to fostering transparency, innovation, and efficiency in governance. Anchored in the broader vision of Digital India and aligned with national data protection regulations, this policy sets forth a comprehensive blueprint for the ethical and secure sharing of government data. The Policy was officially enacted on March 29, 2025, by the Government of Nagaland and represents a transformative step. This policy is designed to create a proactive, open-access platform for disseminating government-generated data derived from public funds. It encompasses data produced by state departments, centrally funded projects and international donor-supported programs, and mandates that all such information be made available in both readable and machine-processable forms. The key features of the policy:

¹⁹⁸ Nagaland State Data Sharing and Accessibility Policy 2024, Government of Nagaland, Gazette Notification No.ST/8-16/11/409 dated 29th March 2025, <https://govtpress.nagaland.gov.in/wp-content/uploads/2025/04/mastercopy.pdf> (Last visited April 03, 2025).

1. The principal aim of the policy is to ensure access to updated data across the electronic network while maintaining alignment with relevant national and state-level legal frameworks.
2. The policy outlines several strategic advantages of promoting widespread access to government-owned datasets. It ensures optimal utilization of publicly funded data, which can enhance citizen welfare. Secondly, it curbs redundant data collection, encouraging inter-departmental data sharing, thus saving time and reducing the cost associated with repetitive data generation. Thirdly, the preparation of a comprehensive data catalogue or metadata will clarify data ownership and improve transparency by helping stakeholders identify and locate existing datasets.
3. The policy emphasizes the adoption of open standards to ensure data interoperability, thereby enabling seamless integration of diverse datasets for comprehensive and cross-sectoral planning.

2.8.1 Data Classification

The Nagaland State Data Sharing and Accessibility Policy 2024 delineates the classification of data sets managed by various government departments. Segregating them into spatial and non-spatial data. This distinction is crucial in establishing the foundation for standardized, metadata, data formats and access policies.

1. Non-spatial data, typically derived from a statistical system, includes structured information such as crop yield or acreage statistics generated by the Directorate of Economic and Statistics. These datasets are primarily produced from census records, government surveys and administrative data collection.

2. Spatial data, on the other hand, encompasses a diverse set of geospatial information, including:

- i. Satellite images
- ii. Aerial photograph
- iii. Topographic and thematic maps.

- iv. GIS (Geographic Information System) analyses.
- v. GPS/DGPA-based map
- vi. Ground-based and crowd-sourced geographic layers.

These spatial datasets are more complex in structure and often require integration with attribute data to be meaningful for applications like urban planning, disaster management, and agricultural development. This emphasizes the importance of standardization, particularly in

- i. Metadata design
- ii. Data formats
- iii. Linking attribute and spatial data
- iv. Developing an accessible public-domain infrastructure through departmental websites.

2.8.2 Legal Frameworks under the Policy

The ownership and legal boundaries for data and information collected by various entities in the state. Key highlights include:

i. Ownership: All data remains the property of the department, organization, agency, or autonomous body that collects it. These entities will host the data in their own IT infrastructure, enabling them to control, share and access.

ii. Legal Integrity: The policy explicitly ensures that access to and sharing of data does not violate any existing laws or regulations of the Government of India. It respects all Acts and legal provisions governing data.

iii. Protection against Misuse: It is clarified that any data shared under this policy cannot be used in legal proceedings as evidence against the government departments.

iv. MOUs for External Sharing: When data is to be shared with Central Agencies or external organizations, it must be done through a Memorandum of Understanding. These MOUs will include a clause allowing the State to use data for its own development, planning and monitoring, ensuring reciprocal utility.

2.8.3. Sharing and Access Protocols

The policy lays down technical and infrastructural mechanisms needed to enable streamlined data sharing across departments and agencies.

i. Centralized Data Infrastructure: It proposes the creation of a state-of-the-art data warehouse with Online Analytical Processing (OLAP) capabilities. This will allow advanced querying, trend analysis, and reporting.

ii. Open Protocol Interface: To ensure interoperability and flexibility, the policy recommends an Open Application Protocol Interface (API) standard. This ensures that various systems can exchange data seamlessly.

iii. Spatial Data Infrastructure (SDI): For managing geospatial data, the policy mandates the formation of a Nagaland Spatial Data Infrastructure (Nagaland- SDI). This SDI would serve as a common platform for sharing data across departments.

iv. Integration and Access: The SDI will be an integral repository that includes data from departments, agencies and automated bodies, functioning as a State Service Delivery Gateway.

v. Supportive Infrastructure: Facilities like the Nagaland Data Centre and the Nagaland State Wide Area Network (NSWAN) will serve as a backbone for achieving seamless data access and sharing.

Thus, the Nagaland State Data Sharing and Accessibility Policy 2024 marks a progressive step towards fostering a data-driven governance system. It protects data ownership while encouraging interoperability through modern technologies. The policy reflects a forward-looking approach to digital governance, enabling informed decision-making, developmental planning, and citizen-centric service delivery in a secure and accountable manner.

2.9 CONCLUSION

The evolution of data protection laws in India, as traced, reveals a gradual yet deliberate transition from rudimentary communication regulations to a sophisticated legislative framework aimed at safeguarding digital personal data. Beginning with colonial-era statutes like the Indian Telegraph Act of 1885 and extending through post-independence legal developments, India's journey has been shaped by growing digitalization and judicial recognition of privacy as a fundamental right. This chapter has meticulously traced the evolution of data protection laws in India, offering a comprehensive overview of the historical, legal and policy-oriented trajectory. They commenced with the rudimentary frameworks of the colonial era, which primarily addressed state surveillance and communication control. Following independence, the Indian legal system gradually adapted to emerging challenges of the information age, culminating in pivotal legislative enactments such as the Information Technology Act 2000 and its subsequent amendments. These early frameworks laid the groundwork for the formal recognition of digital rights and data governance, even though they remained largely reactive and limited in scope. Further, the significant momentum gained during the early 21st century, particularly in response to global digitalization trends and the exponential rise in personal data generation. The inclusion of data protection within the IT (Amendment) Act 2008 and the IT Rules 2011 marked critical steps towards acknowledging the need for safeguarding sensitive personal data. Additionally, the judicial affirmation of the right to privacy as a fundamental right in the landmark Justice Puttaswamy judgment (2017) provided the constitutional foundation necessary for the development of a robust data protection regime.

The deliberation and recommendation of the key expert committee, including the Justice A.P. Shah Committee (2012) and the Justice B.N. Krishna Committee (2018), represented pivotal institutional efforts to formulate a dedicated and contextually relevant data protection Bill between 2018 to 2023. Each successive bill reflects deeper engagements with issues such as individual consent, purpose limitation, data fiduciary accountability, and the role of data protection authorities. The culmination of these legislative efforts is embodied in the Digital Personal Data Protection Act 2023, which aims to harmonize individual privacy rights with the

imperative of innovation, governance, and national security. The forthcoming Digital Personal Data Protection Rule 2025 and region-specific policy measures like the Nagaland State Data Sharing and Accessibility Policy 2024 highlight the growing importance of decentralized and contextual mechanisms in India's federal structure. This chapter establishes that India's approach to data protection has evolved from fragmented statutory provisions into a structured and constitutionally grounded legal framework.

CHAPTER- 3

CONCEPTUAL FOUNDATION AND MULTILAYERED LEGAL FRAMEWORKS FOR DATA PROTECTION IN INDIA

3.1 INTRODUCTION

Data has emerged as a critical asset economically, socially, politically, and individually in an age defined by the digitalization of nearly every aspect of human life. The omnipresence of data in shaping governance, influencing markets, and even determining personal choices underscores the urgent need to understand its nature, regulate its flows and protect its sanctity. As India accelerates its transformation into a digital economy, questions surrounding data protection and privacy no longer remain peripheral concerns; they form the very core of constitutionalism, democratic accountability and human dignity. Data privacy is rooted in liberal constitutionalism, emphasizing the right of individuals to control access to their personal sphere. In contrast, data protection encompasses regulatory mechanisms designed to govern the collection, processing, storage, and transfer of data regardless of consent. The first part of the chapter begins with a fundamental inquiry: what constitutes data in the contemporary landscape? By exploring the diverse typologies, it unpacks the ontological and functional characteristics of data.

Each category of data carries distinct ethical, legal and policy implications when viewed through the lens of emerging technologies like AI, IoT and neurotech. Further analyses the multifaceted risk to data privacy in today's techno-social ecosystem from state surveillance to opaque algorithmic profiling. The proliferation of behavioural surveillance and predictive analytics has not only undermined the consent mechanisms but also introduced new forms of digital vulnerability and exclusion. Amidst these challenges, a range of technological interventions such as encryption, anonymization, blockchain technology, and algorithmic audits can be used as a tool for protecting data integrity. Simultaneously, new forms of rights are

also emerging, which signify a paradigm shift in data governance. The second part of the chapter delves into the legal scaffolding of India's data protection regimes. At its constitutional core lies the recognition of the right to privacy as a fundamental right under Article 21 of the Constitution. This foundational recognition catalyzed the development of statutory and sectoral frameworks like the Digital Personal Data Protection Act 2023 (hereinafter referred to as DPDP Act 2023) and several sector-specific legislations. Yet the Indian regulatory landscape remains complex and fragmented. The lack of horizontal coherence and jurisdictional overlaps creates significant implementation deficits. Equally, the absence of a dedicated independent Data Protection Authority presents institutional gaps that constrain accountability. The final section examines the institutional frameworks and governance models that support the implementation of data laws. It explores the role of MeitY, NIC CERT-In, and NITI Aayog while addressing the institutional voids, such as the absence of a data protection Board.

PART I- DATA AND DATA PRIVACY: CONCEPTUAL FRAMEWORK

3.2 UNDERSTANDING DATA: NATURE, TYPOLOGIES AND CHARACTERISTICS

In the digital age, data functions not only as a technical input but also as a social-legal artefact with profound implications for individual autonomy, commercial innovation, and state power. The evolution of the digital ecosystem has brought with it a diverse taxonomy of data types, each carrying different implications for governance, processing, storage and legal regulation.

3.2.1 Structured, Unstructured and Semi-structured Data

In today's data-driven economy, companies are confronted with data from various sources such as CRMs, web apps, IoT devices, social media, internal systems and third-party APIs. To interpret this information and make better decisions, organizations categorize and manage data into three categories: structured data,

unstructured data and semi-structured data. Each type has different storage options, processing methods and analytics tools¹⁹⁹.

A. Structured Data: Structured data refers to data that is organized in a predefined model or schema, making it easily searchable and processable by algorithms. Structured data is often used in machine learning and drives ML algorithms. Commonly used in banking transactions, census records and health databases, where every element is defined by a fixed attribute, e.g., account number, transaction ID, date, value. These data are easier to manipulate and analyze for general business users with traditional tools.

B. Unstructured Data: Unstructured data is the biggest type of dataset and is typically large, comprising 90% of all enterprise-generated data and it is expanding exponentially with the creation of more digital content. Unstructured data, by contrast, lacks a predetermined organizational format, making it harder to store and analyze. These data are information-rich but hard to process using traditional systems²⁰⁰. It encompasses formats such as images, videos, audio recordings, PDF files, emails, social media posts, or free-form text from chatbots and online reviews²⁰¹. This type of data constitutes a significant majority of global digital information.

C. Semi-structured Data: The semi-structured data represents an intermediate form that retains some level of structure through the use of tags, markers, or metadata but does not conform strictly to relational database models. Examples include XML files, JSON objects, NoSQL databases, email headers, or even log files generated by web servers. This form of data is increasingly common in Internet of Things (IoT) devices, healthcare systems, and e-governance platforms.

¹⁹⁹ Ian Funnell, *Structured Data vs Unstructured Data vs Semi-Structured Data*, Matillion Blog, May 09, 2025, <https://www.matillion.com/blog/what-are-unstructured-structured-and-semi-structured-data-types> (Last visited May. 01, 2025).

²⁰⁰ Alexandra Jonker and Alice Gomstyn, *Structured vs. Unstructured data: What's the difference?*, IBM, Feb 07, 2025, <https://www.ibm.com/think/topics/structured-vs-unstructured-data> (Last visited May 01, 2025).

²⁰¹ Ian Funnell, *Structured Data vs Unstructured Data vs Semi-Structured Data*, Matillion Blog, May 09, 2025, <https://www.matillion.com/blog/what-are-unstructured-structured-and-semi-structured-data-types> (Last visited May. 01, 2025).

3.2.2 Personal, Non-Personal and Sensitive Data

Classifying data into personal, non-personal, and sensitive personal categories is foundational to contemporary data protection frameworks across jurisdictions. These categories are not merely taxonomical; they reflect the level of risk posed to individual rights and determine the degree of regulatory safeguards required for lawful data processing. In the Indian context, particularly under the Digital Personal Data Protection Act 2023, this distinction serves as the legal baseline for assessing obligations to data fiduciaries and rights to data principals. The distinction among these data types is not merely semantic; they form the legal architecture upon which rights, obligations, and liability are structured. Personal and sensitive data invoke an individual rights-based framework, whereas non-personal data increasingly raises questions of community ownership, public good and digital commons.

A. Personal Data: Personal data is generally defined as any data²⁰² about an individual who is identifiable by or related to such data. Section 2(t) of the Digital Personal Data Protection Act 2023, “personal data” refers to “*any data about an individual who is identifiable by or in relation to such data*”. The concept of personal data under Indian law is a pivotal one, especially in the era of digital transformation and data-driven technologies. India’s legal framework on personal data is evolving from sectoral guidelines to comprehensive legislation under the DPDP Act. The definitions vary based on context (health, finance, telecom), but a consistent theme is that any identifiable data about individuals is personal data. It is defined and interpreted across multiple statutes and regulations, reflecting varying degrees of specificity, sectoral focus and privacy concerns. The following is an analysis of how personal data is defined and treated under various Indian laws:

1. Rule 2 (i) under IT Rule 2011²⁰³ was the first attempt at data privacy regulation in India, which defines the term Personal information as “*means any information that*

²⁰² The Digital Personal Data Protection Act 2023 (No 22) § 2(h) “data” means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human being or by automated means.

²⁰³ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, GSR 313(E), Gazette Notification dated 11th April 2011 (India).

relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person”.

2. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016²⁰⁴, under section 2(n), defines “*identity information in respect of an individual, includes his Aadhaar number, his biometric information and his demographic information*”.

3. Supreme Court Judgment: *Justice K S Puttaswamy v Union of India* (2017)²⁰⁵, although it is not a statute, this landmark judgment interpreted Article 21 of the Constitution (Right to life) to include informational privacy. The right to privacy includes the right to control and the dissemination of personal information. Any intrusion must satisfy the *triple test: legality, necessity and proportionality*²⁰⁶. This judgment laid the constitutional foundation for the DPDP Act 2023 and future data privacy norms.

4. Consumer Protection Act 2019²⁰⁷ section 2 (47) defines “*unfair trade practices*” and under clause (x)²⁰⁸ prohibits disclosing personal information given in confidence without consent. Although it does not define data explicitly, it protects consumer data shared during commercial transactions.

B. Non-Personal Data: Non-Personal Data (NPD) refers to data that does not relate to any identified or identifiable individual. This includes anonymized datasets, aggregated statistics, and environmental or industrial data. In 2020, the Ministry of

²⁰⁴ The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, (No 18) Act of Parliament, 2016 (India).

²⁰⁵ Justice K S Puttaswamy (Retd) & Anr. v Union of India & Ors. AIR 2017 SC 4161.

²⁰⁶ Justice K S Puttaswamy v Union of India judgement para-H (page no 277) An invasion of life or personal liberty must meet the threefold requirement of (i) legality, which postulates the existence of law: (ii) need, defined in terms of a legitimate state aim: and (iii) proportionality which ensure a rational nexus between objects and the means adopted to achieve them. https://cdnbbsr.s3waas.gov.in/s3ec0490f1f4972d133619a60c30f3559e/documents/aor_notice_circular/43.pdf (Last visited May 03, 2025).

²⁰⁷ Consumer Protection Act 2019, (No 35) Act of Parliament 2019 (India).

²⁰⁸ Consumer Protection Act 2019, (No 35) § 2 (47) (x) disclosing to other person any personal information given in confidence by the consumer unless such disclosure is made in accordance with the provisions of any law for the time being in force.

Electronics and Information Technology (MeitY) released the Report by the Committee of Experts on Non-Personal Data Governance Framework under the Chairmanship of Kris Gopalakrishnan²⁰⁹, which proposed a new regulatory approach for non-personal data, recognizing it as a valuable economic resource, particularly in AI training and digital innovation. The report categorizes three broad subcategories within non-personal data:

1. **Public non-personal data:** Generated through public infrastructure or government agencies (e.g. Census, weather data)
2. **Community non-personal data:** Derived from groups or communities (e.g. farmer productivity statistics).
3. **Private non-personal data:** Collected by private entities but not identifiable to individuals (e.g. logistics data, market trends).

However, the boundaries between personal and non-personal data are increasingly porous. Through reidentification techniques and data triangulation, anonymized data can often be linked back to individuals, thereby posing latent risks. Hence, non-personal data is no longer immune to privacy concerns and calls for its own ethical and regulatory oversight, especially when processed by dominant tech platforms in opaque ways.

C. Sensitive Personal Data: Sensitive Personal Data (SPD) is a subset of personal data that reveals or is related to attributes that, if mishandled, could cause significant harm to an individual psychologically, physically, or economically. The Justice Srikrishna Committee Reports (2018) outline several categories of SPD, including financial data, health and genetic data, biometric data, sexual orientation, caste, religious or political beliefs²¹⁰. While the DPDP Act 2023 does not explicitly retain a separate legal category of “sensitive personal data”. The high-risk nature of SPD

²⁰⁹ Reports by the Committee of Experts on Non-Personal Data Governance Framework, <https://psa.run/wp-content/uploads/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf> (Last visited on May 03, 2025). The MeitY constituted a Committee of Experts to deliberate on a Data Governance Framework. Office Memorandum No 24(4)/2019-CLES dated 13.09.2019 was issued to create the 8-member committee.

²¹⁰ Report Summary on A Free and Fair Digital Economy, PRS India, <https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy>.

necessitates more robust safeguards. Rule 3²¹¹ of the IT Rule 2011²¹² provides a list of data as Sensitive Personal Data, which includes a password, financial information (bank account, credit card, etc.), health conditions, biometric information, sexual orientation, medical records/history, etc.

3.2.3 Metadata, Big Data, and Inferred Data:

In the evolving architecture of the digital ecosystem, the categorization of data is no longer limited to what individuals explicitly provide. Metadata, Big data and Inferred data are the hidden layers of the digital data ecosystem. Increasingly contemporary data practices involve the generation, extraction, and analysis of metadata, big data and inferred data forms of data that are either derived, ambient or passively generated.

A. Metadata: Metadata refers to ‘*data about data*’²¹³. It describes the context, structure and administrative details of a piece of information rather than its content. It is the invisible infrastructure of digital data. For example, when someone sends an email, the actual message is the content, while metadata would include the sender's IP address, the time sent, the location, file size and device used. In a digital ecosystem, metadata is automatically generated and is critical to sorting, storing, and transmitting information efficiently²¹⁴. Metadata is not always classified as “personal data” unless it is directly identifiable. However, its contextual nature makes it prone to re-identification and algorithmic exploitation, thereby necessitating its inclusion under a broader data protection framework.

B. Big Data: Big data refers to extremely large and complex datasets that comprise structured, unstructured and semi-structured data that continue to grow exponentially

²¹¹ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), r. 3 provided that any information that is freely available or accessible in the public domain or furnished under the Right to Information Act 2005 or any other law for the time being in force shall be regarded as sensitive personal data or information for the purposes of these rules.

²¹² Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, GSR 313(E), Gazette Notification dated 11th April 2011 (India).

²¹³ Annie Badman and Mathew Kosinski, *What is Metadata?*, IBM, 21st Oct 2024, <https://www.ibm.com/think/topics/metadata#:~:text=Metadata%20is%20information%E2%80%94such%20as,for%2C%20organize%20and%20use%20data>. (Last visited May 05, 2025)

²¹⁴ Id.

over time,²¹⁵ and it cannot be processed using traditional database methods. It is characterized by the 5Vs (*volume, velocity, veracity and value*)²¹⁶. These datasets are generated continuously by a variety of sources such as sensors, smartphones, social media, biometric systems, and online transactions and are analyzed using machine learning and artificial intelligence techniques. The distinguishing feature of Big Data is not just its size but its predictive power. It is used to anticipate consumer behaviour, monitor population health, forecast economic trends and even predict criminal activity. However, Big data poses several ethical and legal challenges. Firstly, it often involves secondary uses of the data, data collected for one purpose and may be used for another purpose without the consent of the data owner. Secondly, the aggregation of data when combined across platforms can lead to re-identification even when datasets are anonymized. This undermines the privacy protection.

C. Inferred Data: Inferred data is information generated through analytical processes using algorithms and data models based on existing personal or observed data. Unlike metadata (which is automatically attached to existing data) or big data (which aggregates and processes vast amounts), inferred data is created²¹⁷. For instance, based on a user's Google search history, a system may infer their mental health status. Inferred data is not provided by the data owner, yet it can define them, which raises concerns about individual autonomy, representation and control over one's digital identity.

3.2.4 CHARACTERISTICS OF DIGITAL DATA

Digital data means any kind of information that has been turned into a digital format, whether it's text, images, videos, or financial statements. What makes digital data powerful is how easily it can be shared, stored, reused and analyzed. From an economic perspective, digital data is unique; it's '*non-rival*', meaning multiple people

²¹⁵ *What is Big Data?* Google Cloud, <https://cloud.google.com/learn/what-is-big-data>.

²¹⁶ Annie Badman and Mathew Kosinski, *What is Big Data?*, IBM, 18th Nov 2024, <https://www.ibm.com/think/topics/big-data> (Last visited May 05, 2025).

²¹⁷ Joan M Wrabetz, *What Is Inferred Data And Why Is It Important?*, American Bar Association, Business Law Section, 22nd August 2022, https://www.americanbar.org/groups/business_law/resources/business-law-today/2022-september/what-is-inferred-data-and-why-is-it-important/ (Last visited May 05, 2025).

can use the same data at the same time without running out of it, and ‘*non-excludable*’, which means it’s often hard to stop others from accessing or using it once it gets digitalized. The characteristics of digital data are²¹⁸:

i. Generative: Data isn’t just used once; it keeps generating new data. Every time digital data is used, it can generate new data, insights, or patterns. It’s like a starting point that keeps evolving with each use.

ii. Replicable: Digital data can be copied perfectly and endlessly. Copies are usually identical to the original, making it hard to identify which version came first.

iii. Mixable: Data isn’t stuck in its original context. Information collected for one reason can often be used for another.

iv. Scalable: It’s incredibly cheap to collect and store digital data, so much so that data can grow to massive scales.

v. Storable: It’s often easier to save everything rather than to decide what to keep.

vi. Accessible: It’s available to anyone with internet access.

vii. Persistent: Digital data sticks around potentially forever. Once it’s out there, it’s hard to truly erase.

The core characteristics that distinguish digital data from other data forms are “**5 V’s**” – *volume, velocity, variety, veracity and value*²¹⁹, with *vulnerability* increasingly recognized as a sixth critical dimension in the context of data governance and cybersecurity.

1. Volume: The Explosion of Digital Footprints- Volume refers to the sheer scale and quantity of data generated in a digital environment. With the proliferation of smartphones, IoT devices, social media, sensors, and digital transactions, data is being produced at an unprecedented rate²²⁰. According to an IDC report, the global

²¹⁸ Digital Impact, *The Characteristics of digitized information require us to think carefully about how we use it as a resource*, <https://digitalimpact.io/toolkit/digital-data/characteristics/> (accessed on 8th May 2025)

²¹⁹ Tim Mucci and Cole Stryker, *What is big data analytics?*, IBM, 5th April 2024, <https://www.ibm.com/think/topics/big-data-analytics> (Last visited May 05, 2025)

²²⁰ *Supra* note 218.

datasphere is expected to grow to 175 zettabytes by 2025, as per their 2018 analysis and projections²²¹.

2. Velocity: The Real-Time Pulse of the Digital World- Velocity denotes the speed at which data is generated, transmitted and processed in sectors like fintech, healthcare, and e-commerce. Data flows in real time, updating every second based on transactions, users' behaviour, and system feedback²²².

3. Variety: The Multiplicity of Data Forms and Sources- Variety refers to the diverse types and formats of data, ranging from structured to unstructured formats like audio, video, images, social media content and natural language inputs. This diversity complicates not only data storage and processing but also its legal classification²²³.

4. Veracity: Trustworthiness and Accuracy of Data - Veracity deals with the truthfulness, reliability and quality of data. Inaccurate, incomplete or manipulative data can lead to harmful consequences, especially in automated systems like algorithmic decision making²²⁴.

5. Value: The Economic Importance of Data- Data is often described as the 'new oil', although it functions more like infrastructure than a commodity. Its value lies in how it is aggregated, processed, and applied²²⁵. In both the private and public sectors, data enables targeted marketing, social analytics, predictive governance, and algorithmic innovations. Corporations extract immense value through behavioural insights. The economic value of data raises issues of ownership, monopolization, and public interest use, making it a key subject of data sovereignty.

6. Vulnerability: The Exposure to Risk and Exploitation- Vulnerability refers to the inherent risks associated with digital data, particularly its susceptibility to unauthorized access, misuse, breaches, and manipulation.

²²¹ David Reinsel, John Gantz and John Rydning, *The Digitalization of the World From Edge to Core*, IDC release a white paper with the support of Seagate, Nov 2028, <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf> (Last visited May 05, 2025).

²²² *Supra* note 219.

²²³ *Supra* note 219

²²⁴ *Supra* note 219.

²²⁵ *Supra* note 219.

3.3 DATA PROTECTION AND DATA PRIVACY: LEGAL AND CONCEPTUAL DISTINCTION

The terms '*data protection*' and '*data privacy*' are often used interchangeably; however, from a legal and conceptual point of view, these two terms are distinct in scope, orientation, and normative foundation. While closely related, data protection is primarily a regulatory construct concerned with the systems and conditions governing the processing of data, whereas data privacy is rooted in constitutional and human rights jurisprudence, focusing on individual autonomy, dignity and informational self-determination. Data privacy refers to the individual's right to control how their personal information is collected, used, stored and disclosed²²⁶. It is a manifestation of the broader right to privacy, which encompasses personal informational and decisional autonomy. In the Indian legal landscape, the right to privacy was explicitly recognized as a fundamental right in the judgment of Justice K S Puttaswamy (Retd) v Union of India (2017), where a nine-judge bench of the Supreme Court unanimously held that privacy is intrinsic to life and liberty under Article 21 of the Constitution. In contrast, data protection is a regulatory and institutional mechanism that governs the collection, processing, storage, transfer, and erasure of personal data.

While privacy is a normative ideal, data protection is the instrumental framework that helps realize this ideal in practice. At the core, data protection is about establishing legal obligations for data fiduciaries and enforceable rights for data subjects²²⁷. It encompasses a set of principles such as Lawfulness, fairness and transparency, Purpose limitation, Data minimization, Storage limitation, Security safeguards, Accountability and redress mechanisms. The Digital Personal Data Protection Act 2023 embodies these principles by articulating duties of data fiduciaries, establishing grounds for lawful processing, and providing rights to data

²²⁶ Sh Manoj Roy Sarkar, *The Evolving Landscape of Digital Privacy in India: Balancing Innovation and Data Protection by the Government*, Data Protection and Data Privacy by INTERNATIONAL CENTRE FOR INFORMATION SYSTEMS AND AUDIT, PursuIT, 9th Edition, e-Journal, 2024, [https://cag.gov.in/uploads/icisa_virtual_publishing/Journal-with-cover-DG-message-08-10-2024-06704c77f434894-](https://cag.gov.in/uploads/icisa_virtual_publishing/Journal-with-cover-DG-message-08-10-2024-06704c77f434894-25842653.pdf#:~:text=Data%20privacy%20refers%20to%20the%20protection%20of,limiting%20unauthorized%20access%20or%20use%20by%20others.(Last%20visited%20May%2008,%202025))

25842653.pdf#:~:text=Data%20privacy%20refers%20to%20the%20protection%20of,limiting%20unauthorized%20access%20or%20use%20by%20others.(Last visited May 08, 2025)

²²⁷ *What is Data Protection and Privacy?*, Clodian, <https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/> (Last visited May 08, 2025).

principals and setting up regulatory authorities for compliance and enforcement. Despite their conceptual distinction, data protection and data privacy are not mutually exclusive; rather, they are complementary and interdependent. **Privacy is the goal, while protection is the method.** Without effective data protection laws, privacy rights become unenforceable and illusory.

3.4 RISKS AND THREATS TO DATA PRIVACY RIGHTS

In the contemporary digital ecosystem, the protection of privacy has become increasingly complex. Despite evolving jurisprudence that recognizes privacy as a fundamental right, especially after the Puttaswamy judgment in India, individuals remain constantly exposed to privacy risks arising from various actors. The most critical and recurring threats to data privacy in India and globally include state surveillance, corporate exploitation, cyberattacks and predictive behavioural profiling.

3.4.1 State Surveillance

State surveillance represents one of the most enduring and controversial threats to privacy rights. Governments have historically justified surveillance on the grounds of national security, public order, and law enforcement, yet such activities often escape effective judicial and legislative oversight. In India, legal authorization for surveillance is primarily derived from Section 5(2)²²⁸ of the Indian Telegraph Act 1885²²⁹- *“Power of the Government to take possession of licensed telegraph and to order interception of message”* and Sections 69 and 69A of the Information

²²⁸ The Indian Telegraph Act 1885, (No 13) § 5(2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order.

²²⁹ The Indian Telegraph Act, 1885 (No. 13) Act of Parliament, 1885, (India).

Technology Act, 2000²³⁰ - “Power to issue directions for interception or monitoring or decryption of any information through any computer resources”²³¹ and “Power to issue directions for blocking for public access of any information through any computer resource”²³².

Section 69A empowers the Central Government to direct the blocking of public access to online information if deemed necessary for India’s sovereignty, security, public order or foreign relations. Such action must be justified in writing and may involve intermediaries or government agencies executing the blocking order. In the case of *Manohar Lal Sharma v Union of India & Others*,²³³ advocate Manohar Lal Sharma filed a PIL before the Supreme Court of India in response to an explosive allegation made by international media and Amnesty International under the “Pegasus Project”²³⁴. These reports suggested that the Pegasus spyware, developed by the Israeli company NSO Group, had been used to conduct illegal surveillance on Indian citizens, including journalists, political leaders, activists, judges, and election strategists. On October 27, 2021, the Supreme Court ordered the formation of an independent Technical Committee to investigate the matter. The committee submitted its report in July 2022. The Supreme Court has not yet issued a final ruling based on the report; this case has become a significant milestone in the legal discourse around digital surveillance, privacy and state accountability in India²³⁵.

3.4.2 E-Commerce and Social Media

Digital platforms, particularly e-commerce websites and social media companies, are major vectors of privacy erosion. Unlike traditional surveillance, the threat here is commercial rather than governmental. The rise of the digital economy has made

²³⁰ The Information Technology Act 2000 (No. 21) Act of Parliament. 2000 (India).

²³¹ The Information Technology Act 2000 (No. 21) § 69- Power to issue directions for interception or monitoring or decryption of any information through any computer resources.

²³² The Information Technology Act 2000 (No. 21) § 69A, Act of Parliament, 2000 (India).

²³³ *Manohar Lal Sharma v Union of India & Others*- W.P (Crl) No 000314-2021 filed on 26-07-2021.

²³⁴ Pegasus Spyware Probe, Supreme Court Observer, <https://www.scobserver.in/cases/manohar-lal-sharma-prime-minister-pegasus-spyware-probe-case-background/> (Last visited May 8, 2025).

²³⁵ *Manohar Lal Sharma v Union of India & Others*, Privacy Library, NLU Delhi, <https://privacylibrary.ccgnlud.org/case/manohar-lal-sharma-vs-union-of-india-and-ors> (Last visited May 8, 2025).

personal data a new currency of the digital economy. In this model, users are not just customers, they are the product too. Their personal preferences, routines, and affiliations are commodified through data extraction practices that operate at scale and with minimal accountability. Popular platforms like Facebook (Meta), Amazon, Google, and Instagram routinely track users across devices and platforms using cookies, devices, fingerprinting, and app permissions. These platforms collect vast amounts of data from users to drive targeted advertising, behavioural prediction, and content manipulation²³⁶.

- Voluntarily shared information (e.g., name, email, gender, phone number)
- Automatically captured metadata (e.g., IP address, geolocation, device ID)
- Observed behaviour (e.g., click patterns, scroll speed, purchase history)
- Inferred and predictive interests (based on AI and machine learning models)

Moreover, algorithmic feeds on platforms like YouTube and TikTok often amplify sensational or emotionally manipulative content based on users' profiles, contributing to an echo chamber and political polarization²³⁷. Users often face a '*take it or leave it*' scenario where using essential services means giving up privacy. This leads to exhaustion from constant consent requests and gradually undermines an individual's sense of control over their own choice.

3.4.3 Data Breach and Cyber Attacks

With ubiquitous connectivity and data-driven governance, cyberattacks have emerged as potent threats to individual privacy and national security. Data breaches and cyberattacks represent direct, tangible threats to privacy rights. The exposure of sensitive personal and financial information to unauthorized entities leads to identity theft, financial fraud, and reputational damage. According to the ITU Global

²³⁶ Zara Amir, *How to Manipulate your Ad Algorithm*, Evolve Dash Blog, 31st Dec 2024, [https://evolvedash.com/blog/understanding-ad-algorithms/#:~:text=In%20the%20digital%20age%2C%20advertising,gather%20data%20from%20various%20sources,\(Last visited May 8, 2025\)](https://evolvedash.com/blog/understanding-ad-algorithms/#:~:text=In%20the%20digital%20age%2C%20advertising,gather%20data%20from%20various%20sources,(Last%20visited%20May%208%2C%202025).).

²³⁷ Varuntorn, *How Social Media Algorithms Shape Public Opinion*, Media & Society, 8th April 2025, <https://mediaandsociety.org/2025/04/08/how-social-media-algorithms-shape-public-opinion/>.

Cybersecurity Index 2021, India ranks 10th globally²³⁸, but still India has witnessed major breaches in recent years in 2020, the Aadhaar database was reported to have suffered multiple unauthorized accesses. In 2021, Air India, Domino's and the CoWIN vaccine portal were reportedly compromised, leading to unauthorized data breaches affecting millions of users²³⁹. These threats reveal a systemic failure to prioritize data protection practices in India. The scale of cyber threats has expanded exponentially in recent years. According to the Cybersecurity Ventures Report 2023, the global cost of cybercrime is projected to reach \$8 trillion in 2023, and is expected to hit \$10.5 trillion annually by 2025²⁴⁰.

3.4.4 Predictive Profiling and Behavioural Manipulation

Predictive profiling and behavioural manipulation represent some of the most insidious, opaque, and under-regulated threats to digital privacy in the 21st century. These practices involve the use of data-driven inference techniques and algorithmic models to anticipate, influence, and even shape an individual's future behaviour, preferences, and decisions²⁴¹. Predictive profiling refers to the use of AI and machine learning systems to analyze a large volume of historic data, social media activity, browsing history, purchase patterns, search terms, location data and even biometric data to generate individual or group profiles. Predictive profiling often bypasses the consent of the individual and relies on inferred data (data not provided but derived), thus falling outside many legal protections. In case of Behavioural Manipulation, once profiles are created, they are deployed in behavioural targeting systems that seek to

²³⁸ International Telecommunication Union, *Global Cybersecurity Index 2020 Measuring Commitment to Cybersecurity*, ITU Publications, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf, (Last visited May 10, 2025).

²³⁹ Himanshi Singh, "CoWIN Data Breach", Cyber Peace, Jun 17, 2023, <https://www.cyberpeace.org/resources/blogs/cowin-data-breach>, accessed on (10th May 2025)

²⁴⁰ Mitangi Parekh, "Cybersecurity Ventures Report on Cybercrime", Esentire, July 23, 2024, <https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime#:~:text=Cybercrime%20Growth,%2C%20and%20post%20Dattack%20recovery.&text=Cybersecurity%20Ventures%20attributes%20this%20growth,approach%20to%20avoid%20business%20disruption.> (accessed on 10th May 2025).

²⁴¹ *What is predictive analytics?*, IBM, Aug 8, 2022, <https://www.ibm.com/think/topics/predictive-analytics> (accessed on 10th May 2025)

manipulate users' actions through micro-targeted content²⁴², e.g., Nudge²⁴³ (only 1 seat left at this price). Its aim is not simply to predict but to alter decision-making autonomy.

3.5 TOOLS AND TECHNOLOGIES FOR DATA PROTECTION

In the contemporary digital ecosystem, legal norms alone are insufficient to ensure sound data protection. As data flows become transitional, real-time, and algorithmically processed, there is a growing consensus that technological interventions must work in tandem with legal frameworks to safeguard privacy, autonomy, and informational self-determination. The convergence of privacy-enhancing technologies such as anonymization, encryption, and blockchain technology and algorithmic auditing mechanisms has emerged as an effective response to the rising tide of data exploitation and systemic surveillance. The key technologies that are increasingly being integrated into privacy-by-design strategies.

3.5.1 *Anonymization and Pseudonymization of data*

Anonymization involves removing or altering personal identifiers from datasets such that individuals can no longer be identified, directly or indirectly²⁴⁴. In contrast, pseudonymization “*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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*”.²⁴⁵ Pseudonymization replaces private identifiers with fictitious labels or keys, making re-identification possible only with additional information held separately. These

²⁴² Marcello Ienca, *On Artificial Intelligence and Manipulation*, Topoi 42 (2023), pp 833-842, DOI: <https://doi.org/10.1007/s11245-023-09940-3>, (Last visited May 12, 2025).

²⁴³ *Nudge marketing is a selling technique that requires manipulating customer behaviour to close more deals. Makers use psychological insights to speed up clients' decision-making process*, <https://sendpulse.com/support/glossary/nudge-marketing>.

²⁴⁴ *Guidance Note: Guidance on Anonymisation and Pseudonymisation*, Data Protection Commission, June 2019, <https://www.dataprotection.ie/sites/default/files/uploads/2022-04/Anonymisation%20and%20Pseudonymisation%20-%20latest%20April%202022.pdf>.

²⁴⁵ Council Regulation 2016/679, 2016 O.J. (L 119) 1, art. 45 (EU).

methods are foundational to privacy-preserving data analytics, allowing institutions to process data while minimizing the risk to individual privacy. The report published by the Ministry of Electronics and Information Technology on India AI 2023²⁴⁶, emphasizes secure data sharing frameworks for India's AI ecosystem. It highlights the need for anonymization and pseudonymization to protect individuals' privacy. These techniques ensure that data used for AI research or public platforms like the India Dataset Platform (IDP) does not compromise personal privacy.

3.5.2 Encryption and Homomorphic Encryption of Data

Encryption is the process of transforming readable data into an unreadable format, ensuring that only authorized parties can access the information²⁴⁷. It is a cornerstone of data confidentiality, widely used in securing communication, cloud storage, and digital financial transactions. Whereas, Homomorphic encryption, a more advanced form, allows computation on encrypted data without decrypting it. This ensures that sensitive data remains protected even during processing, making it ideal for cloud-based AI, health research, and federated analytics²⁴⁸.

3.5.3 Blockchain Technology and Smart Contract

Blockchain technology ensures immutability, transparency, and decentralization of data²⁴⁹, it can be defined as *“Blockchain is a type of distributed ledger, comprised of digitally recorded data in packages called blocks which are linked together in chronological order in a manner that makes the data very difficult to alter once recorded, without the alteration of all subsequent blocks and a majority of the network*

²⁴⁶ MeitY, *India AI 2023 First Edition by Expert Group*, Ministry of Electronics and Information Technology, October 2023, <https://indiaai.s3.ap-south-1.amazonaws.com/docs/IndiaAI+Expert+Group+Report-First+Edition.pdf>.

²⁴⁷ *What is encryption?* Google Cloud, <https://cloud.google.com/learn/what-is-encryption> (Last visited May 12, 2025).

²⁴⁸ IEEE Digital Privacy, *What is Homomorphic Encryption?* <https://digitalprivacy.ieee.org/publications/topics/what-is-homomorphic-encryption/>, (Last visited May 15, 2025).

²⁴⁹ Stephanie Susnjara and Ian Smalley, *What is blockchain?*, IBM, <https://www.ibm.com/think/topics/blockchain> (Last visited May 15, 2025).

colluding together”²⁵⁰. It records transactions across multiple nodes in a tamper-resistant way. So when it is applied to data protection, it can facilitate transparent data consent logs²⁵¹, time-stamped records of access and modification and decentralized identity management systems. Smart contracts²⁵² are self-executing code embedded within the blockchain that enforce that predefined terms and conditions are met²⁵³. For data protection, smart contracts can automate users' consent, trigger alerts for data access and ensure compliance in real-time.

3.5.4 Algorithmic Impact Assessment (AIA)

An Algorithmic Impact Assessment (AIA) is a regulatory and procedural tool designed to evaluate the risks, fairness, and transparency of algorithmic systems, particularly in an automated decision-making context. “*Algorithmic Impact assessments are a mechanism for enabling accountability of an algorithm by assessing the possible societal impact of an algorithmic system before the system is in use*”²⁵⁴. AIA requires organizations to document (i) the purpose of the algorithm, (ii) the type of data used, (iii) potential harms and (iv) mitigation strategies. In an age of predictive profiling, AIA’s help regulators and the public pre-emptively assess harms²⁵⁵.

²⁵⁰ Winston Maxwell and John Salmon, *A Guide to blockchain and data protection*, Hogan Lovells, Nov 2018, https://digital-client-solutions.hoganlovells.com/_uploads/blockchain-insights/5649DataProtection-BlockchainPaperARTWORKSTAGE3Low-res-gumfy.pdf.

²⁵¹ *Adapting Consent Management to Decentralized Data Ecosystems*, Secure Privacy, Mar 26, 2025, <https://secureprivacy.ai/blog/decentralized-data-consent-management>.

²⁵² Smart contracts use blockchain technology. The term is used to describe computer program code, maintained on the various “nodes” constituting a blockchain network that is capable of facilitating executing and enforcing the negotiation or performance of an agreement upon the occurrence of pre-defined conditions.

²⁵³ *What are Smart Contracts on blockchain?* IBM, <https://www.ibm.com/think/topics/smart-contracts> (Last visited on May 15, 2025).

²⁵⁴ *Algorithmic Impact Assessment: User Guide*, Ada Lovelace Institute, Feb 8th, 2022, <https://www.adalovelaceinstitute.org/resource/aia-user-guide/#fnref-21> (Last visited on May 15 2025).

²⁵⁵ *Algorithm Charter for Aotearoa New Zealand, Algorithm Impact Assessment User Guide*, New Zealand Government, Dec 2023, <https://www.privacy.org.nz/assets/Privacy-Week-2025/Headliners-Resource-Pack/Algorithm-Impact-Assessment-guide-Algorithm-Charter-for-Aotearoa-New-Zealand.pdf> (Last visited on May 15, 2025)

3.6. DATA PROTECTION REGIME: NEW WAVE OF RIGHTS

As personal data becomes an increasingly valuable asset in the digital economy, the conception of privacy rights is undergoing a major transformation. Traditional notions of privacy as mere non-interference are no longer sufficient. Instead, what is emerging is a new generation of data rights dynamics. The new generation of data rights, including the right to be forgotten, data portability, and objection to automation, reflects a shift from passive privacy to participatory digital citizenship, with algorithmic fairness.

3.6.1 Right to be Forgotten

The Right to be Forgotten enables individuals to request the deletion of personal data when it is no longer necessary, has been unlawfully processed, or when consent has been withdrawn. This right finds its most prominent articulation in Article 17 of the EU General Data Protection Regulation, which enshrines the ‘*right to erasure*’²⁵⁶. The Digital Personal Data Protection Act 2023 does not mention the right to be forgotten, but provides a limited right to erasure. However, its implementation depends on future rules and the discretion of the Data Protection Board. In India, before the enactment of the Digital Personal Data Protection Act 2023, various High Courts have upheld the right to be forgotten in specific cases involving sensitive personal information. For example, in the case of *Jorawar Singh Mundy @Jorawar Singh Mundy v Union of India and Ors*²⁵⁷ the court directed Google, Lex. in and Indian Kanoon to remove the judgment till further order. Kerala High Court in the case of *Sredharan T v State of Kerala*²⁵⁸ recognizes the ‘*right to be forgotten*’ as a part of the right to privacy. In *V vs High Court of Karnataka*²⁵⁹, the Karnataka High Court recognizes the right to be forgotten. The Orissa High Court in the case of *Subranshu Raot v State of Odisha*²⁶⁰ held that the right to be forgotten is a remedy for the victim

²⁵⁶ Council Regulation 2016/679, 2016 O.J. (L 119) 1, art. 17 (EU), 17 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.

²⁵⁷ *Jorawar Singh Mundy v Union of India and Ors* WP (C) 3918/2021 & CM Appl 19941/2021.

²⁵⁸ *Sredharan T v State of Kerala* WP (C) No. 9478 of 2017.

²⁵⁹ *V v High Court of Karnataka*- 2017 SSC Online Kar 424.

²⁶⁰ *Subranshu Raot v State of Odisha* WP (C) 4159/2020

of sexually explicit videos or photos on social media. In the case of *Zulfiqar Ahmed Khan v Quintillion Business Media Pvt Ltd*²⁶¹, the Delhi High Court supported individuals' right to be forgotten.

3.6.2. Right to Data Portability

The right to data portability allows individuals to receive their data in a structured, machine-readable format and to transfer it to another service provider. It promotes user autonomy, platform competition and data ownership²⁶². In the EU GDPR, Article 20²⁶³ provides a legal mandate for portability, particularly for data provided by the data subject. The Digital Personal Data Protection Act 2023 does not explicitly mention portability, missing a key opportunity to enable users to exit platform monopolies or reclaim data sovereignty. Portability is not just about moving data; it also enables users to reclaim control from data monopolies and break digital dependencies.

3.6.3 Right to Object to Automated Decision-Making

Automated decision-making systems use algorithms to make or significantly influence decisions about individuals. The right to object to such decisions is crucial to preserving individual autonomy and procedural fairness²⁶⁴. Under Article 22²⁶⁵ of the GDPR, individuals have the right not to be subject to decisions based solely on

²⁶¹ *Zulfiqar Ahmed Khan v Quintillion Business Media Pvt Ltd* CS (OS) 642/2018.

²⁶² OECD, THE IMPACT OF DATA PORTABILITY ON USER EMPOWERMENT, INNOVATION, AND COMPETITION 2 (2024), https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/the-impact-of-data-portability-on-user-empowerment-innovation-and-competition_ee329380/319f420f-en.pdf.

²⁶³ Council Regulation 2016/679, 2016 O.J. (L 119) 1, art. 20 (EU)- Right to Data Portability (1) the data subject 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.

²⁶⁴ Elena Abrusci and Richard Mackenzie-Gray Scott, *The Questionable Necessity of a New Human Right Against being Subject to Automated Decision-Making*, Vol 31, Issue 2, INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY, 2023, pp 114-143, DOI: <https://doi.org/10.1093/ijlit/eaad013>, (Last visited May 17, 2025).

²⁶⁵ Council Regulation 2016/679, 2016 O.J. (L 119) 1, art. 22 (EU)- Automated Individual Decision-Making Including Profiling- (1) The data subject 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.

automated processing. The Digital Personal Data Protection Act 2023 does not provide this right, despite India's rapid adoption of ADM systems in various sectors. This represents a regulatory gap, particularly as India's digital welfare infrastructure expands.

3.6.4 Right to Redressal and Algorithmic Fairness

The Right to redress ensures that individuals have an accessible and effective pathway to seek a remedy when their data rights are violated. In the digital context, this extends to errors in profiling, data breaches, or algorithmic discrimination. Algorithmic fairness, meanwhile, refers to the principle that decision-making systems must be transparent, non-discriminatory, and accountable. This includes fairness in data selection, auditing AI models for bias, and ensuring explainability and inclusivity²⁶⁶.

3.7 RELEVANCE OF DATA PROTECTION IN THE INDIAN CONTEXT

As India transitions into a digital economy, the need for a rights-based and technologically adaptive data protection regime becomes not merely desirable but indispensable. From Aadhaar-linked public services to UPI-led financial inclusion to deep tech ventures in AI and biotech, India's digital transformation is redefining the relationship between individual, state and the market. In this context, personal data is no longer just an asset, it is the substrate of economic value, social classification and political control. India's digital journey is profound but uneven; in this landscape, a robust data protection framework is not a luxury; it is the precondition for ethical governance, digital trust, and social justice.

3.7.1 Rise of The Digital Economy

India's digital economy is expanding rapidly through government initiatives like Digital India, Make in India and Startup India. As per the report of the Economic Times, *"India to be \$ 1 Trillion digital economy by FY 28: IT minister Rajeev*

²⁶⁶ Niklas Kossow, Svea Windwehr and Mathew Jenkins, *Algorithmic Transparency and Accountability*, Transparency International, Feb 2021, https://knowledgehub.transparency.org/assets/uploads/kproducts/Algorithmic-Transparency_2021.pdf

Chandrasekhar”²⁶⁷. As per the “*State of India Digital Economy Report 2023*”²⁶⁸, India’s digital economy has rapidly expanded. The country has embraced Digital Public Infrastructures like Aadhar, UPI, and CoWIN to enable inclusive digital governance and financial access. While internet penetration and mobile broadband use have soared, digital divides persist across rural-urban and state lines. However, concerns around privacy, infrastructure inequality and data security. Today, among all countries in the world, India is the country with the highest digital transactions, accounting for nearly 46% share, as per the 2022 data²⁶⁹. This digital surge, however, exposes vast amounts of personal data to diverse actors like banks, apps, government databases, and AI engines. With a robust data protection regime, this growth can lead to systemic exploitation, profiling and exclusion. To understand this in depth, four interlinked dimensions are illustrated to show how India’s digital economy amplifies the need for strong data governance.

i. Deep Digitalization of Informal Sectors: India’s digitalization is no longer confined to the urban or formal sector. It is reaching deep into the informal rural enterprise, street vendors, small stores, gig workers and daily wage earners. Tools like UPI, Aadhaar-linked payments, and the e-SHRAM portal are helping these groups connect to formal financial and digital systems, boosting inclusion and efficiency. However, this shift also means their work and personal data are being captured and analyzed without clear consent or protection. The rapid datafication of livelihood raises urgent concerns about privacy, ownership and informed digital participation.

ii. Digital Platforms and Monopolistic Data Aggregation: India’s digital economy is increasingly shaped by a few powerful tech giants like Google, Amazon, Meta, Jio, Flipkart and Paytm. These platforms are no longer just service providers; they have

²⁶⁷ The Economic Times, “India to be \$1 trillion digital economy by FY28: IT Minister Rajeev Chandrasekhar, ET May 21, 2024, <https://economictimes.indiatimes.com/tech/technology/india-to-be-1-trillion-digital-economy-by-fy28-it-minister-rajeev-chandrasekhar/articleshow/110302464.cms> (Last visited May 17, 2025).

²⁶⁸ State of India’s Digital Economy Report 2023, ICRIER Prosus, Centre for Internet and Digital Economy, Feb 2023, https://icrier.org/pdf/State_of_India_Digital_Economy_Report_2023.pdf.

²⁶⁹ India’s UPI: A Global front-runner in digital payment status, PIB Thiruvananthapuram, Oct 30, 2023, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1973082#:~:text=UPI%20is%20used%20at%20all,China%2C%20Thailand%20and%20South%20Korea.> (Last visited May 17, 2025).

become gatekeepers controlling access to market information and digital services. Their dominance allows them to shape everything from how we search online to how ads are shown and even how creditworthiness is judged. What makes this more complex is their ability to collect massive amounts of behavioural data, often across different products and services. For example, what we search on Google, buy on Amazon, or pay for using Paytm can all feed into a single user profile. The algorithms that power these platforms often operate like black boxes; users don't know how decisions are made, which creates a lack of transparency. There's also the risk of surveillance where our habits become a tool for profit.

iii. Cross-Border Data Flows and Digital Trade: As India becomes a key player in the global digital economy, cross-border data flows are now at the heart of its integration into cloud services, outstanding fintech, health tech, and supply chain analytics. Indian startups and industries rely on real-time global data exchange to innovate and stay competitive. However, without proper regulation, this can lead to data colonization where sensitive data about Indian users is stored and analyzed and monetize in a foreign jurisdiction. This undermines data sovereignty, limits local control over critical digital assets, and raises serious concerns about privacy, national security, and fair value distribution from India's growing digital footprint.

iv. Deep Tech and Data Dependency: India is investing heavily in IA, biotechnology and smart infrastructure, all of which rely on large-scale, high-quality datasets. Initiatives such as IndiaAI²⁷⁰ (AI for All), NDHM (National Digital Health Mission) are designed to transform governance and service delivery. These innovations are deeply data-driven, often prioritizing data collection over individual rights. As a result, health records are being profiled without consent, AI systems are reinforcing social biases in welfare distribution or policing and widespread biometric surveillance via drones and CCTVs. Without strong privacy safeguards, these tools risk eroding trust and reinforcing systemic inequalities in the digital age.

²⁷⁰ NITI Aayog, *National Strategy For Artificial Intelligence # AI For ALL*, June 2018, <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf>.

3.7.2 Privacy Concerns and Citizens' Autonomy

The digital transformation of public and private life in India has redefined how individuals relate to the state, the market, and even their own digital identities. Yet, this transformation has brought with it a growing and under-addressed set of concerns fundamentally around the erosion of citizens' autonomy, cognitive liberty and mental self-determination. The four interconnection dimensions of how digital technologies affect privacy and autonomy in the Indian context are:

i. Behavioural Surveillance and Manipulative Technologies: Modern digital infrastructures are built not merely to observe, but to shape behaviour. Behavioural surveillance goes beyond monitoring; it predicts and guides future actions through targeted advertising, push notifications, algorithmic curation, and interface design (*called dark patterns*)²⁷¹. The Digital Personal Data Protection Act 2023 is largely silent on manipulative tech or algorithmic nudging and provides no meaningful redress for behavioural profiling or emotional influence.

ii. Privacy of Thoughts and Neurological Data: Emerging neuro technologies such as brain-computer interfaces (BCIs) pose an unprecedented risk to mental privacy. This includes not only data about brainwaves or moods but also predictive inference of thoughts, attention levels, or even intent. The ability of machines to read and respond to cognitive signals can lead to a violation of cognitive liberty, especially when deployed in school, the workplace or by the state²⁷². The collection and processing of personal data through such devices raises significant concerns about moral and psychological effects, potential risks and the security of the data involved.

iii. Household Surveillance: Smart speakers connected to TVs, security cameras, and voice assistants have transformed the home into data-rich surveillance zones. In India, growing affordability of devices like Amazon Echo, Google Nest and security

²⁷¹ Dharmender Jhamb, *Dark Patterns Pose a Growing Concern in India's Digital Landscape*, The Hindu, <https://www.thehindu.com/business/Industry/dark-patterns-pose-a-growing-concern-in-indias-digital-landscape/article68634686.ece> (Last Updated September 12, 2024, 07:18 PM IST).

²⁷² Prof Dr Phil et al, *The Protection of Mental Privacy in the Area of Neuroscience, Societal, Legal and Ethical Challenges*, European Parliamentary Research Service, July 2024, [https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU\(2024\)757807_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU(2024)757807_EN.pdf).

cameras has led to an uptick in domestic surveillance. Most devices default to cloud storage, raising cross-border privacy and data ownership concerns.

3.7.3 Human Rights Implications

In the age of ubiquitous digital infrastructure, questions of data protection extend beyond privacy and sovereignty to the very core of human rights and personhood. The digital shift has reconfigured long-standing legal categories such as identity, autonomy, and accountability. These transformations do not merely complement human rights frameworks; they actively challenge them, introducing new forms of exclusion, manipulation and injustice. The crucial and underexamined human rights dimensions of the data-driven paradigm in India and globally are:

i. Digital Identity and Statelessness: Digital identity systems, such as Aadhaar, promise inclusion, portability, and efficiency in public service delivery. However, when access to rights and entitlements depends on biometric authentication, identity becomes unstable. Without a verifiable digital identity individual risks being denied access to services. Moreover, systems reliant on biometric authentication may inadvertently disenfranchise users due to technical errors or mismatches. In such instances, digital identity does not serve as a means of empowerment but rather contributes to a new form of digital statelessness²⁷³.

ii. Deepfake and Violation of Digital Personhood: The rise of deepfake technology, which is AI-generated synthetic media that can fabricate voices, faces, and videos, poses an existential threat to digital personhood and reputational integrity. In India, deepfakes have been weaponized for misinformation campaigns, image-based sexual abuse, particularly targeting women, political defamation and impersonation. These violations are not just technological, they strike at the core of dignity, consent, and the right to truth. In India, while criminalizing voyeurism and cyberstalking, it lacks the framework to address non-consensual synthetic media, leaving victims digitally

²⁷³ Sustainability Directory, *Statelessness in Digital Age and Human Rights?*, Sustainability Directory, Apr 15, 2025, <https://prism.sustainability-directory.com/scenario/statelessness-in-digital-age-and-human-rights/s> (Last visited May 18, 2025).

vulnerable. Ethical implication is that an AI-mediated data ecosystem being seen no longer means being a reality that endangers both private reputation and public trust.

iii. Environmental Justice and Data: The OECD's Digital Economy Paper 2024²⁷⁴, recommendation on ICT and the Environment, highlights the urgent need to reassess the environmental impact of digital technologies. It identifies three layers of environmental impact from digital technologies: direct effects like energy consumption and emissions from infrastructure, enabling effects such as improved efficiency in sectors like transport and agriculture, and systemic effects, including behavioural shifts like increased remote work. The ICT sector has expanded significantly, growing three times faster than the broader economy, with internet users rising from 2 billion in 2010 to 5.3 billion in 2022. However, this growth brings mounting challenges. Global data centers alone consumed between 240-340 TWh of electricity in 2022, and the sector now accounts for up to 4% of global greenhouse gas emissions. The increasing demand for AI, particularly deep learning and generative models, is driving up compute needs and intensifying energy and water consumption. Moreover, the environmental toll of mining rare minerals for digital devices, along with the global e-waste crisis, is worsening. The report urges governments to integrate digital and environmental strategies more closely, embracing circular economy principles, investing in green digital skills and updating measurement tools²⁷⁵.

PART II: MULTILAYERED LEGAL REGULATORY FRAMEWORKS ON DATA GOVERNANCE

3.8 Constitutional Provisions

The evolution of digital society has brought with it profound questions about the nature and boundaries of fundamental rights in India. In particular, as data becomes central to governance, commerce, and identity, the Indian Constitution must serve not

²⁷⁴ OECD, *Review of Relevance of the OECD Recommendation on ICTS and the Environment*, OECD Digital Economy Paper, Nov 2024 No. 370, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/11/review-of-relevance-of-the-oecd-recommendation-on-icts-and-the-environment_ebd374ec/216766c6-en.pdf.

²⁷⁵ Id 274.

as a legal safeguard but also as a moral framework that guides how the individual relates to the state and the digital ecosystem. The recognition of privacy as a fundamental right under Article 21 has opened new constitutional frontiers where dignity, informational autonomy and technological governance intersect. This section explores the constitutional underpinnings of data protection in two vital and interrelated areas: (i) Article 21 and Right to Privacy, (ii) the tension between Right to Privacy and the Right to Information and the emerging constitutional principles of dignity, autonomy and informational self-determination. The Indian Constitution offers more than legal protection; it offers a vision of justice in the age of algorithms and data capitalism.

3.8.1 Article 21 of the Constitution of India: The Bedrock of Digital Privacy

Article 21 guarantees the right to life and personal liberty. Over time, judicial interpretation has enriched this provision to include a wide array of human rights education, health, clean environment and many other aspects to live a dignified life and now privacy. In the landmark case of *Justice K S Puttaswamy v Union of India (2017)*, the Supreme Court unanimously declared that the right to privacy is an integral part of Article 21, affirming that life and liberty are meaningless without the freedom to control personal information. This was not a mere doctrinal shift; it was a recognition that in a world where individuals are constantly being profiled, tracked, and algorithmically influenced, privacy is foundational to human dignity and democracy. The Court introduced a structured test of legality, necessity and proportionality to assess any infringement on this right. This framework not only restrains state surveillance but also creates an obligation for the state to ensure data protection mechanisms, especially where private actors wield power over personal information. Thus, Article 21 now acts as a constitutional shield against arbitrary data collection, unauthorized surveillance, and disproportionate use of biometric and algorithmic systems. It urges both the legislature and judiciary to build a jurisprudence of digital justice grounded in liberty, not just legality.

3.8.2 Constitutional Conflicts: Right to Information v Right to Privacy

One of the most nuanced constitutional challenges in the digital era is balancing the *Right to Information* (RTI) under the Right to Information Act 2005²⁷⁶ with the *Right to Privacy*. On the surface, these two rights may seem to clash; RTI promotes transparency and accountability of public institutions, while privacy protects the individual's personal space. However, the conflict is not binary; it is contextual. For instance, seeking details of a public servant's attendance or financial disclosure may serve the public interest, but demanding their medical records or Aadhaar number may violate their privacy. The Supreme Court in the case of *Girish Ramchandra Deshpande v Central Information Commission*²⁷⁷ (2013), the Supreme Court examined whether personal details of a public servant, such as employment records, asset declaration, income tax returns, or disciplinary actions, could be withheld under section 8(1)(j)²⁷⁸ of the RTI Act 2005. The Court ruled that such information qualifies as personal and is protected from disclosure unless a larger public interest clearly justifies it. It emphasized that an employee's performance and service details are private matters between the individual and their employer, and making them public without cause would amount to an unwarranted invasion of that person's privacy.

In *R K Jain v Union of India*²⁷⁹ (2013), the Supreme Court ruled that details from a public servant's Annual Confidential Report (ACR), including related notes and correspondence, could be withheld under Section 8(1)(j) of the RTI Act as they constitute personal information. This view was reaffirmed in *Canara Bank v C S Shyam*²⁸⁰ (2018), where the Courts denied access to an employee's personal records, citing a lack of overriding public interest. Both decisions upheld the earlier ruling in *Girish Deshpande* emphasizing that unless there is a clear public interest, personal details of employees are protected from disclosure under the RTI Act. This tension

²⁷⁶ The Right to Information Act 2005 (No 22), Act of Parliament, 2005 (India).

²⁷⁷ *Girish Ramchandra Deshpande v Central Information Commission* (213) 1 SCC 212

²⁷⁸ The Right to Information Act 2005 (No 22) § 8(1)(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.

²⁷⁹ *R K Jain v Union of India* (2013) 14 SCC 794.

²⁸⁰ *Canara Bank v C S Shyam* (2018) 11 SCC 426.

becomes even more pronounced in the digital sphere, where RTI filings can lead to mass disclosure of personal data, especially when data is stored in interoperable government platforms.

3.9. SECTOR-SPECIFIC REGULATIONS- HEALTH SECTOR

3.9.1 *Draft Health Data Management Policy 2022*

The Draft Health Data Management Policy 2022²⁸¹ under the Ayushman Bharat Digital Mission (ABDM), marks a transformative moment in India's attempt to constitutionally align health data governance with the fundamental right to privacy recognized in the Justice KS Puttaswamy judgement. Rooted in the principle of “*privacy and security by design*”, the policy builds an architecture for the National Digital Health Ecosystem (NDHE), explicitly avoiding the centralization of sensitive health data. The policy lies in a consent-based framework which vests full control in the data principal. Consent²⁸² under this framework must be free, informed, specific, and clearly expressed, ensuring data subjects retain autonomy over their digital health identities²⁸³. The policy also enumerates robust privacy rights empowering data principals to seek access, request portability, object to processing, and obtain confirmation of how and where their data is used. Data fiduciaries are obliged to facilitate these rights transparently and without procedural hurdles. To institutionalize these safeguards, the policy mandates the appointment of a Data Protection Officer and a Chief Information Security Officer (CISO). These officers are responsible for compliance, audit and breach response mechanisms. Further, Clause 29 strictly governs the sharing of anonymized or de-identified data, primarily for research purposes. Policy affirms the principle of non-exclusion, ensuring that no citizen is denied healthcare for refusing to participate in the NDHE.

²⁸¹ Draft Health Data Management Policy 2022, April 2022, Version 02. National Health Authority, https://abdm.gov.in:8081/uploads/Draft_HDM_Policy_April2022_e38c82eee5.pdf.

²⁸² Consent has the same meaning as set out under Section 14 of the Indian Contract Act 1872.

²⁸³ Draft Health Data Management Policy 2022, April 2022, Version 02, Clause 9

3.9.2 *Medical Termination of Pregnancy (Amendment) Act 2021*

The Medical Termination of Pregnancy (MTP) Act 1971, as amended in 2021²⁸⁴ it is a crucial piece of legislation that not only safeguards reproductive rights but also ensures important data privacy protections for women seeking abortions in India. Although the Act does not explicitly frame its provisions in terms of ‘*data protection*’, it implicitly recognizes the importance of confidentiality. The 2021 Amendment to the Act, while expanding access to safe abortions, also strengthens privacy safeguards. The newly inserted Section 5A²⁸⁵ explicitly mandates that the identity and personal details of the women undergoing abortion must not be revealed to anyone except persons authorized by law. Breach of this confidentiality provision is punishable with imprisonment up to one year, thereby embedding a criminal sanction to enforce medical privacy²⁸⁶.

3.9.3 *Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act 1994*

The Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act 1994²⁸⁷, enacted to curb the misuse of the potential diagnostic technique for sex selection. While its principal aim is to prevent female feticide, it imposes strict confidentiality obligations on medical professionals and diagnostic establishments. Section 5 of the Act mandates that no prenatal diagnostic techniques may be conducted without written consent from pregnant women. Furthermore, the women must be informed of all known side effects, risks, and limitations, implicitly affirming the principle of informed consent, which is a foundational element of modern data protection law. Additionally, Section 29 explicitly requires that records be kept secure, preserved for two years, and disclosed only to authorized authorities.

²⁸⁴ The Medical Termination of Pregnancy (Amendment) Act 2021, (No 8), Act of Parliament, 2021.

²⁸⁵ The Medical Termination of Pregnancy (Amendment) Act 2021, (No 8), § 5A (1) No registered medical practitioner shall reveal the name and other particulars of a women whose pregnancy has been terminated under this Act except to a person authorized by any law for the time being in force.

²⁸⁶ The Medical Termination of Pregnancy (Amendment) Act 2021, (No 8), § 5A(2).

²⁸⁷ The Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act 1994 (No 57) Act of Parliament, 1994 (India).

These confidentiality obligations extend to diagnostic laboratories and genetic counselling clinics, making them legally liable for any breach of data security.

3.9.4 *Mental Healthcare Act 2017*

The Mental Healthcare Act 2017²⁸⁸ it is a landmark legislation that not only foregrounds the rights of persons with mental illness but also introduces robust protections for informational privacy and confidentiality. At its core, Section 23²⁸⁹ of the Act guarantees every person the right to confidentiality about their mental health, mental healthcare treatment, and physical healthcare. This protection is further strengthened by Section 25, which grants individuals the right to access basic medical records of their mental health. Moreover, Section 14 allows patients to designate a ‘nominated representative’ who can make decisions regarding treatment and data disclosure when the individual is incapacitated.

3.10 SECTOR-SPECIFIC REGULATIONS- FINANCIAL & BANKING

3.10.1 Reserve Bank of India

The Reserve Bank of India (RBI), as India’s central banking institution, plays a pivotal role in shaping not only the country’s monetary policy but also the governance of financial data ecosystems. Over the last decade, the RBI has evolved from being a traditional regulator to a digital watchdog, issuing a series of circulars, master directions, and guidelines that collectively create a robust framework for data privacy and protection in India’s financial sector.

1. Reserve Bank of India (Digital Lending) Directions 2025

The Reserve Bank of India (Digital Lending) Direction 2025 with operational and compliance, represents a critical regulatory effort to tame the unchecked proliferation

²⁸⁸ The Mental Healthcare Act 2017, (No 10), Act of Parliament, 2017 (India).

²⁸⁹ The Mental Healthcare Act 2017, (No 10), § 23 Right to confidentiality. (1) A person with mental illness shall have the right to confidentiality in respect of his mental health, mental healthcare, treatment and physical healthcare.

of digital lending platforms while embedding data privacy and consumer protection principles into India's financial technology ecosystem. These Directions²⁹⁰ act as a rights-based correction to the data extractive practices of the past, especially where digital borrowers were often subjected to opaque data harvesting and algorithmic profiling. A defining feature of the Directions is the explicit consent requirement. Regulated Entities (REs) and their Lending Services Providers (LSPs) must obtain verifiable, prior, and express consent from borrowers before collecting any personal data. This includes sensitive data such as contact list, media, location or biometric identifiers²⁹¹. Notably, the Directions categorically prohibit blanket consent or forced app permission, reiterating the constitutional principle of informational autonomy. The guidelines require that the Borrowers must be given a clear choice when it comes to their personal data. They should have the right to give or deny consent for specific data use, limit who it is shared with, control how long it's retained, and even withdraw consent at any point²⁹². If requested, the lending entity or service provider must delete the borrower's data. At every interaction, the reason for collecting consent must be clearly explained²⁹³. Additionally, personal information should only be shared with third parties if the borrower has explicitly agreed to it²⁹⁴. Additionally, personal information should only be shared with third parties if the borrower has explicitly agreed to it, unless required by law or regulatory obligations. Regulated Entities (REs) must ensure that any Lending Service Providers (LSPs) they work with only store

²⁹⁰ The Reserve Bank of India (Digital Lending) Directions 2025, RBI/2025-26/36. DOR.STR.REC.19/21.07.001/2025-26 dated May 8th, 2025, (these Directions shall come into force immediately except for ¶ 6, which shall come into effect from November 1, 2025, and para 17, which shall come into effect from June 15, 2025) <https://website.rbi.org.in/documents/87730/39710850/DirectionsonDigitalLending.pdf>.

²⁹¹ The Reserve Bank of India (Digital Lending) Directions 2025 Clause 12. Collection, usage and sharing of data with third parties (i) RE shall ensure that any collection of data by their DLA and DLA of their LSP is need-based and with prior and explicit consent of the borrower having audit trail. In any case, RE shall also ensure that DLA of RE/LSP desist from accessing mobile phone resources like file and media, contact list, call logs, telephony functions, etc. A one-time access can be taken for camera, microphone, location or any other facility necessary for the purpose of on-boarding/KYC requirements only, with the explicit consent of the borrower.

²⁹² The Reserve Bank of India (Digital Lending) Directions 2025 Clause 12(ii) The borrower shall be provided with an option to give or deny consent for use of specific data, restrict disclosure to third parties, data retention, revoke consent already granted to collect personal data and if required, make the RE/LSP delete/forget the data.

²⁹³ The Reserve Bank of India (Digital Lending) Directions 2025 Clause 12(iii) the purpose of obtaining borrowers' consent needs to be disclosed at each stage of interface with the borrowers.

²⁹⁴ The Reserve Bank of India (Digital Lending) Directions 2025 Clause 12(iv).

essential borrower information like name, address, and contact details, and nothing more. The full responsibility for data privacy and protection lies with the RE²⁹⁵. They must have clear policies on what data can be stored for how long, how it can be used, and how it should be destroyed, along with breach-handling protocols²⁹⁶. These policies must be clearly shared on both the REs' and LSPs' websites. Biometric data must not be collected or stored unless legally permitted²⁹⁷. All consumer data must be stored on servers within India. If processed abroad, the data must be erased there and moved back to the Indian server within 24 hours²⁹⁸.

2. Master Direction on Digital Payment Security Controls (2021)

One of the most progressive frameworks, this direction, Master Direction on Digital Payment Security Controls²⁹⁹ mandates regulated entities (REs), including banks and non-banking financial companies, to schedule Commercial Banks excluding RRBs, Small Finance Banks, Payment Banks and Credit Card issuing NBFCs, to implement an end-to-end protection mechanism for the digital payment infrastructure. It requires encryption of sensitive payment data and secure user authentication. These guidelines require mobile applications should avoid saving personal or login information like user IDs, passwords, encryption keys, or security codes directly on the user's device. Instead, they must ensure that such data is clear and secure from memory as soon as the user exits the app, protecting the user from potential misuse or data breaches³⁰⁰. This aligns with principles of privacy by design and purpose limitation, foundational in data protection regimes.

²⁹⁵ The Reserve Bank of India (Digital Lending) Directions 2025, Storage of Data, Clause 13 (i).

²⁹⁶ The Reserve Bank of India (Digital Lending) Directions 2025, Storage of Data, Clause 13 (ii).

²⁹⁷ The Reserve Bank of India (Digital Lending) Directions 2025, Storage of Data, Clause 13(iii).

²⁹⁸ The Reserve Bank of India (Digital Lending) Directions 2025, Storage of Data, Clause 13(iv).

²⁹⁹ Master Direction on Digital Payment Security Controls, Reserve Bank of India, RBI/2020-21/42, DoS.CO.CSITE.SEC NO. 1852/31.01.015/2020-21 dated February 18, 2021, <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD7493544C24B5FC47D0AB12798C61CDB56F.PDF>. (Last visited May 21, 2025).

³⁰⁰ Master Direction on Digital Payment Security Controls, Reserve Bank of India, RBI/2020-21/42, Clause 63- The mobile application should not store/retain sensitive personal/consumer authentication information such as IDs, passwords, keys, hashes, hard coded references on the device and the application should securely wipe any sensitive customer information from memory when the customer/user exits the application.

***3. RBI Circular on Storage of Payment System Data (2018)*³⁰¹**

In recent times, there has been considerable growth in the payment ecosystem in the country. Such systems are highly technology-dependent, which necessitates the adoption of safety and security measures. This circular, often referred to as the “*data localization mandate*”, directs all payment system operators to ensure that all payment-related data of Indian users is stored only in systems located within India. The circular serves a dual purpose: sovereign control over data and enhanced accountability in case of breaches or misuse.

4. Master Direction on Information Technology Framework for NBFCs (2017)

The Master Direction of Information Technology Frameworks³⁰² recognizes that financial data held by NBFC (Non-Banking Finance Company) is personal, sensitive and commercially valuable and hence demands robust IT governance, cybersecurity protocols, and data access restrictions. NBFCs must also conduct periodic audits and maintain a risk management plan mechanism, critically to uphold informational integrity and confidentiality. The purpose of Information Security (IS) is to control access to sensitive information, ensuring use only by legitimate users so that data cannot be read or compromised without proper authorization³⁰³.

3.10.2 State Bank of India

As India’s largest public sector bank, the State Bank of India serves over 50 crore³⁰⁴ customers and handles a vast volume of financial, biometric, and personally identifiable data on a daily basis. While the SBI is not governed by a dedicated ‘SBI Privacy Act’, it operates within a layered framework of regulatory norms and internal

³⁰¹ RBI Circular on Storage of Payment System Data, RBI/2017-18/153, DPSS.CO.OD.NO. 2785/06.08.005/2017-2018 dated 6th April 2018, <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF> (Last visited on May 21, 2025).

³⁰² Reserve Bank of India, Master Direction—Information Technology Framework for the NBFC Sector, RBI/DNBS/2016-17/53 (June 8, 2017), <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD53E0706201769D6B56245D7457395560CFE72517E0C.PDF>. (Last visited on May 21, 2025).

³⁰³ Information and Cyber Security, Clause 3. Information Security.

³⁰⁴ <https://sbi.co.in/web/about-us/about-us>, (Last visited May 21, 2025).

policies that collectively ensure the privacy and protection of consumer data. SBI, as a Regulated Entity (RE), is bound by the Reserve Bank of India's key directives on data protection, like Digital Lending Guidelines³⁰⁵, Master Direction on Information Technology³⁰⁶, and the Circular on Storage of Payment System Data³⁰⁷, etc.

1. Bank Policy on Record and Data Retention (version 1.0)³⁰⁸

The Policy is to guide and implement standard procedures for record/ document storage, retrieval and disposal of all important documents, including documents to be preserved as per statutory/ regulatory requirements. Data originated/ owned by the Bank, as well as data obtained from an external source, will be under the scope of this Policy. The key clause that reflects SBI's commitment to ethical data stewardship, aligning internal practice, is as follows:

i. Scope and Applicability (Clause 7): Establishes that the policy applies to all physical and digital records of the Bank, covering data created, processed and stored by domestic offices or branches.

ii. Mode of Retention and Preservation (Clause 8): The documents specified in the Annexure to the Policy include Physical form (hard copy), Electronic/ digital or digitalized form/ scanned copy (soft copy) or in both. The documents should be preserved in such a way that ensures that there is no tampering, alteration, destruction, or anything which endangers the context, authenticity, utility or accessibility of the Document.

iii. Duration of Retention: Prescribe that the records at Branches, Administrative Office, Local Head Office, GITC, etc. will be retained for the period as mentioned in

³⁰⁵ *Supra* note 290.

³⁰⁶ *Supra* note 302.

³⁰⁷ *Supra* note 301.

³⁰⁸ Bank's Policy on Record and Data Retention (version 1.0), SBI Organisational Planning and Systems & Procedures Department, Corporate Centre, Mumbai, January 2024, <https://sbi.co.in/documents/17836/37002821/230224-Bank%27s+Policy+on+Record+and+Data+Retention.pdf/c243eef8-8233-9df1-d052-633c8b732422?t=1708671581287>, (Last visited on May 21, 2025).

Annexure. However, data can be retained longer under special circumstances like a suit filed, fraud cases, disciplinary cases, etc.

iv. Classification of Records: Records are classified based on sensitivity and regulatory importance, such as KYC, transactional data, audit reports with distinct retention periods and confidentiality protocols, ensuring data minimization and risk-based retention.

2. SBI Online Privacy Policy

The State Bank of India publishes a detailed Privacy Policy³⁰⁹ on its digital platform, which articulates how the bank collects, processes, shares, and stores user data. The policy emphasizes:

- Consent-driven data collection.
- Use of personal data strictly for banking or legally permitted purposes,
- No sales or unauthorized sharing of customer data with third parties.

This policy, though not statutory, reflects an institutional recognition of the right to informational privacy, particularly in response to rising public concern over data misuse in the digital banking space

3.10.3 Securities and Exchange Board of India

The Securities and Exchange Board of India (SEBI), as the principal regulator of India's securities and capital markets, has increasingly incorporated data privacy and protection norms. Within its legal and supervisory architecture. While SEBI does not administer a standalone privacy statute, its regulations, circulars, and codes of conduct reflect a maturing understanding of data security, investors' confidentiality and data fiduciaries' responsibilities.

³⁰⁹ State Bank of India, Privacy Policy, https://www.onlinesbi.sbi/sbijava/Privacy_Statement.html#:~:text=We%20follow%20best%20security%20practices,to%20confidential%20information%20about%20you.&text=SBI%20does%20not%20release%20customer,or%20as%20per%20your%20mandate. (Last visited May 21, 2025).

1. Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs) 2024

To strengthen the cybersecurity measures in the Indian security market and to ensure adequate cyber resiliency against cybersecurity incidents/ attacks, the Cybersecurity and Cyber Resilience Frameworks (CSCRF)³¹⁰ for SEBI REs has been formulated in consultation with the stakeholders. The key objective of CSCRF is to address evolving cyberattacks, to align with industry standards, to encourage efficient audits, and to ensure compliance by SEBI REs. The Cyber Resilience Goal of the framework proposes layering of Full-disk Encryption (FDE) along with File-based Encryption (FE), which will be used for data protection³¹¹. The CSCRS has provisions to address ‘harvest now- decrypt later’ attacks through continuous risk assessment and adoption of robust data protection measures. Data security measures under the framework requires organizations to ensure data security, organizations must manage information in line with their strategy, protecting its confidentiality, integrity, and availability.

Regulated Entities (REs) must use strong encryption for both data-at-rest and data-in-transit, and Market Infrastructure Institutions (MIIs) are encouraged to explore encryption during data processing. Data must be classified, stored securely within India, and remain accessible and readable. Additionally, REs must maintain adequate capacity and implement robust tools to prevent data leaks and unauthorized disclosure³¹². The CSCRF gives directions to all REs to stay informed about and follow cybersecurity and data protection laws issued by SEBI and the Government of India: REs shall enforce effective data protection measures³¹³. This ensures their systems and practices align with national legal and regulatory standards.

³¹⁰ Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs), Securities and Exchange Board of India, Aug 20, 2024, Circular no: SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113, <https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-85964.html> (Last visited on May 21, 2025).

³¹¹ Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs), Cyber Resilience Goal.

³¹² Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs), clause 3.3 PR. DS: Data Security.

³¹³ Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs), PR.AT: Guidelines (PR.DS.S4).

3.11 SECTOR-SPECIFIC REGULATIONS- TELECOMMUNICATIONS

India's telecom sector, regulated by the Department of Telecommunications and the Telecom Regulatory Authority of India (TRAI), plays a critical role in handling volumes of personal data and sensitive data. As per the TRAI Press Release No. 44/2025, dated 29th May 2025, the number of active wireless subscribers in April 2025 was 1072.73 million³¹⁴. After the report of CloudSEK that hackers were allegedly selling a massive 1.8 terabyte database containing the sensitive details of 750 million Indian mobile users on the dark web. The compromised data is believed to include highly sensitive personal data, raising serious concerns about data privacy, cybersecurity, and potential misuse of citizens' information³¹⁵. In the case of *Nivedita Sharma v Bharathi Hexcom Ltd*³¹⁶ the Hon'ble Consumer Dispute Redressal Commission (NCDRC) reaffirms that the relentless flood of telemarketing messages and the unauthorized sharing of customer data by telecom operators with other parties amounts to a clear violation of privacy. The judgment stressed that sharing personal data without customer consent, especially with insurers and financial institutions, is not just unethical but legally wrong. It underscored the urgent need for strong data protection practices by telecom service providers to safeguard consumer rights.

1. *The Telecommunication Act 2023*

The Telecommunication Act 2023³¹⁷ Section 28 prohibits sending a '*specified message*' which includes offers, advertisements or promotions related to goods, services, jobs, property, or investments, regardless of their legality or authenticity, without user consent. The law requires telecom operators to obtain prior user consent, maintain a DO Not Disturb (DND) register, and provide a tool for users to report spam

³¹⁴ Telecom Regulatory Authority of India, Press Release No. 44/2025, Dated 29th May 2025, https://www.trai.gov.in/sites/default/files/2025-05/PR_No.44of2025_0.pdf.

³¹⁵ *Cybersecurity Firm Claims Data Leak of 750 Million Telecom Users, Dot Asks Telcos For Security Audit*, Economic Times Telecom, <https://telecom.economictimes.indiatimes.com/news/industry/cybersecurity-firm-claims-data-leak-of-750-million-telecom-users-dot-asks-telcos-for-security-audit/107244949#:~:text=With%20the%20personal%20information%20of,Security%20Research%2C%20Sparsh%20Kulshrestha%20said> (Updated On Jan 30, 2024, at 08:00 AM IST).

³¹⁶ *Nivedita Sharma v Bharathi Hexcom Ltd*, Appeal no 52 of 2012.

³¹⁷ The Telecommunication Act 2023, (No 44), Act of Parliament, 2023 (India).

or malicious messages. It mandates an online grievance redressal system to ensure users can easily raise and resolve complaints.

2. *Telecom Commercial Communications Customer Reference (Second Amendment) Regulations 2025*

Clause 22 of the Telecom Commercial Communications Customer Reference (Second Amendment) Regulations 2025³¹⁸ requires strict internal safeguards to prevent the misuse of AI/ML-based detection systems, ensuring that subscriber data remains secure. These controls are crucial for maintaining data privacy and ensuring complete compliance with existing data protection laws and regulatory standards governing the use of such technologies.

3.12 CODE OF PRACTICES, ETHICAL GUIDELINES FOR DATA PROTECTION

1. National Ethical Guidelines for Biomedical and Health Research Involving Human Participants

The ICMR guidelines (2017), National Ethical Guidelines for Biomedical and Health Research Involving Human Participants³¹⁹ rooted in the principle of informed consent, confidentiality, and purpose limitation. The guidelines mandate

- Voluntary, informed consent for data collection in research,
- De-identification or anonymization of data,
- Prior ethical approval.

These guidelines apply to all biomedical, social and behavioural science research for health conducted in India involving human participants, their biological material and data.

³¹⁸ Telecom Commercial Communications Customer Reference (Second Amendment) Regulations 2025, Telecom Regulatory Authority of India, Notification dated 12th February 2025, https://www.trai.gov.in/sites/default/files/2025-02/Regulation_12022025.pdf.

³¹⁹ National Ethical Guidelines for Biomedical and Health Research Involving Human Participants, Indian Council of Medical Research, (2017) https://ethics.ncdirindia.org/asset/pdf/ICMR_National_Ethical_Guidelines.pdf.

2. *Online Gaming Norms:* The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rule 2021³²⁰ Platforms must prevent games that cause user harm, publish clear KYC, refund, and deposit policies, and ensure real-money games display a visible verification mark. Robust grievance redressal, user identity checks, and protections against addiction and child harm are now compulsory.

3. *IRDAI Guidelines on Information and Cyber Security (2023)*

Insurance Regulatory Development Authority of India Guidelines on “Information and Cyber Security 2023”³²¹ apply to all Insurers, including Foreign Re-Insurance Branches (FRBs) and Insurance Intermediaries regulated by the IRDAI. As per the guidelines, data includes all types of data created, received or maintained by the regulated entities. Guidelines provide a “*Contractual Clause on Data Privacy*” for data retention. The organisation shall ensure that it retains the “Exclusive” right to data ownership throughout the agreement.

PART III- INSTITUTIONAL ARCHITECTURE FOR DATA GOVERNANCE

3.13 KEY INSTITUTIONS FOR DATA GOVERNANCE

India’s evolving data privacy and digital governance landscape is supported not just by laws and policies but also by a constellation of specialized institutions that execute, monitor, and advise on issues of cybersecurity, data protection, digital infrastructure and public accountability. The five pivotal institutions, each playing a distinct yet complementary role in shaping India’s data governance ecosystem, are:

³²⁰ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rule 2021, GSR 139 (E) (India), 2021, <https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf> (Last visited May 22, 2025).

³²¹ Information and Cyber Security Guidelines, Insurance Regulatory Development Authority of India, April 2023, <https://irdai.gov.in/document-detail?documentId=1354286> (Last visited May 22, 2025).

3.13.1 Ministry of Electronics and Information Technology (MeitY)

MeitY serves as the nodal ministry for all digital and data governance policies in India. It is the architect behind key frameworks such as the Information Technology Act 2000, Information Technology Rules 2011 and 2012 and the Digital Personal Data Protection Act 2023. Its responsibilities include framing rules for data privacy, overseeing the functioning of digital platforms, and fostering innovation through policy instruments like Digital India.

3.13.2 Indian Computer Emergency Response Team (CERT-In)

CERT-In is India's national cybersecurity incident response agency functioning under MeitY. It plays a frontline role in detecting, reporting, and mitigating cyber threats and issues, frequently issuing advisories, alerts and guidelines to public and private sector entities. Its role in mandating breach reporting, maintaining logs of critical data, and supporting investigations makes it central to real-time data protection and crisis management.

3.13.3 National Informatics Centre (NIC)

The NIC is the technical backbone of India's e-governance infrastructure. It plays a crucial role in securing personal data collected through public digital services. It is closely associated with the government in different aspects of governance by establishing a nationwide state-of-the-art ICT infrastructure and services for the Central Government, State Governments, UT administration, Districts and other Government bodies.

3.14 GAPS AND CHALLENGES IN INDIAN LEGAL FRAMEWORKS

Despite significant legislative strides, most notably through the Digital Personal Data Protection Act 2023 and the IT laws and sector-specific regulations, India's data governance architecture continues to face several systemic and structural challenges. These are:

i. Absence of horizontal application: One of the most significant limitations in India's data protection regime is its vertical or sector-specific nature, wherein obligations often apply only to state actors or regulated private entities. However, horizontal application, i.e., uniform privacy obligations across all entities (including private corporations, tech startups, and civil society actors) remains elusive. This means that while a telecom provider is bound by strict privacy rules under TRAI, a social media platform or health-tech startup may operate under weaker or ambiguous regulatory oversight.

ii. Jurisdictional Conflicts: The data flow is inherently borderless, but Indian law remains largely territorial in nature. This creates jurisdictional tensions both within the country and internationally. Internationally, issue arises when data of Indian citizens is stored or processed outside India, where Indian authorities may lack legal control. For example, if a data breach occurs in a cloud server hosted in another jurisdiction, enforcing Indian privacy law becomes complex.

iii. Consent Fatigue: Modern data privacy regimes are built around the ideal of informed consent, but in practice, this model is showing serious signs of strain. With the sheer volume of digital services, users are bombarded with frequent, lengthy, and often incomprehensible consent requests. This leads to a phenomenon known as “*consent fatigue*”, where users mechanically click “*accept*” without understanding the implications.

iv. Enforcement and Institutional Deficits: Even the most well-drafted legislation is ineffective without credible enforcement mechanisms. India currently suffers from a lack of adequately resourced, independent enforcement bodies. While the Data Protection Board of India has been proposed under the DPDP Act 2023, its composition, powers and independence remain a subject of concern, given the potential for executive influence. Without a strong institutional infrastructure, the right to privacy risks becoming illusory, recognized on paper but not operationalized in practice.

3.15 EMERGING AREAS OF CONCERN

As India advances towards a data-driven society, the terrain of privacy, ethics, and data justice is evolving rapidly. While traditional legal frameworks have focused on regulating digital platforms, telecom services, and financial data, emerging technologies and infrastructure pose new multidimensional challenges. These emerging areas demonstrate that data governance is no longer confined to server rooms and courtrooms. It now shapes human dignity, ecological justice, and democratic integrity. Some emerging areas of concern are:

i. AI, Predictive Policing and Social Scoring: The integration of Artificial Intelligence in governance, particularly in predictive profiling, facial recognition and social credit-style scoring, poses a significant threat to civil liberties and due process. Without clear legal boundaries and democratic oversight, these technologies risk automating discrimination and normalizing surveillance under the guise of efficiency.

ii. Environmental Costs and Data Infrastructure: Behind every data transaction lies a physical infrastructure of data centres, server farms, and energy-intensive cooling systems. The environmental impact of digital consumption is often overlooked in privacy and tech policy databases. These infrastructures contribute to carbon emissions and resource depletion, which raise concerns about environmental sustainability.

iii. Neurotechnology and Mind Privacy: The rise of neurotechnology devices that decode brain signals, predict thoughts or enable brain-computer interaction raises the frontier question of ‘*mental privacy*’. If thoughts can be accessed, interpreted, or manipulated by a machine, existing privacy laws become obsolete.

3.16. CONCLUSION

The evolution of data protection in India reflects a deepening awareness of the transformative power and potential perils of the digital age. This study attempts to lay down a structural understanding of the conceptual and regulatory foundations that inform India’s approach to data governance. By dissecting the various classifications

of data, from structured and unstructured to sensitive and inferred, it becomes evident that the value of data lies not only in its volume or velocity, but in its ability to shape decisions, influence behaviour, and impact rights. India's trajectory from constitutional recognition to the passage of the Digital Personal Data Protection Act 2023 shows a promising yet unfinished commitment to safeguarding informational autonomy in both state and private domains. There is a growing recognition that protecting data is no longer just a technical or legal issue. It is fundamentally about preserving democratic values in an increasingly digitalized society. While India has laid a substantial foundation for data protection through a composite legal and institutional framework, significant normative, structural, and operational gaps persist. In this context, this chapter examined a range of contemporary tools, including anonymization, encryption, blockchain, and algorithmic impact assessments, positioning them as critical enablers in a techno-legal ecosystem that fosters user empowerment and systemic accountability. The analysis of emergent data rights, such as the right to be forgotten, data portability, and objection to automated decision-making, reflects an evolving right-based framework that reclaims individual agency in the digital sphere. Lastly, the chapter highlighted a series of emerging concerns, such as predictive policing, the environmental cost of data infrastructure, and neurotechnology, which demand urgent legal attention.

CHAPTER -4

INTERNATIONAL LEGAL FRAMEWORKS ON DATA PRIVACY AND DATA PROTECTION

4.1 INTRODUCTION

In an increasingly digitalized and interconnected world, the movement of data across borders has become both a necessity and a concern. As personal data travels globally, facilitating commerce, governance, innovation, and communication, it also traverses a fragmented landscape of legal regimes. While national legislation often reflects domestic political and cultural values, international frameworks aim to reconcile divergent normative approaches, seeking common standards in an otherwise heterogeneous legal environment. The significance of international legal frameworks lies in their potential to harmonize diverse national regulations, promote mutual trust in cross-border data transfer, and embed privacy as a global public good. These frameworks also offer essential guardrails against abuses by both state and non-state actors, particularly in domains like surveillance, algorithmic profiling and AI governance.

The impetus for international corporations in this domain arises from the complex realities of cross-border data processing, surveillance practices, and global tech platforms whose operations rarely align neatly with national jurisdictions. Against this backdrop, instruments such as the General Data Protection Regulation (GDPR) of the European Union, the Organisation for Economic Co-operation and Development (OECD) Guidelines, the Council of Europe's Convention 108+, and the recent UN initiatives on digital trust and human rights represent significant, albeit varying, efforts to articulate coherent and enforceable norms of data protection. These instruments serve not only as legal texts but also as normative anchors that influence legislative developments worldwide. This chapter undertakes a doctrinal and comparative analysis of these international instruments, mapping their principles,

scopes of application, enforcement mechanisms, and conceptual underpinning. It seeks to explore the extent to which these frameworks promote harmonization, protect fundamental rights and adapt to the fast-evolving digital economy. Special focus is laid on the normative conflicts between data sovereignty and international interoperability, between human rights and state or corporate interests, and between hard law and soft law approaches in international data governance. To understand the regional divergence and convergence in data governance regimes, this chapter examines selected jurisdictions from each continent, chosen for their representative legal models or emerging regulatory relevance.

1. European Continent: The European Union's General Data Protection Regulation (GDPR) is considered the most influential and comprehensive framework globally, setting high benchmarks for privacy rights.

2. North America: From North America, California was selected for its pioneering California Privacy Right Act (CPRA), often seen as a U.S. counterpart to the GDPR.

3. South America: From South America, Canada offers a mature privacy regime with federal and provincial coordination under the Personal Information Protection and Electronic Documents Act, providing insights into federal governance models.

4. African Continent: South Africa was studied for the African continent, as its Protection of Personal Information Act (POPIA) makes a significant regional effort towards GDPR-aligned legislation.

5. Asia: From Asia, South Korea was selected for its robust Personal Information Protection Act (PIPA) and strong enforcement record, demonstrating a proactive regulatory stance.

6. Neighbouring countries: China was studied to assess how regional geopolitics and varying levels of digital maturity influence data protection frameworks around India.

Furthermore, to understand how data privacy is regulated across these countries, ten key aspects were considered, including each country's legal philosophy and

constitutional basis for privacy. The strength and scope of enforcement mechanisms and the rules governing international data transfers. The analysis also covers surveillance and national security exceptions, algorithmic decision-making transparency, and the alignment with digital trade and innovation. Additional focus areas include emotional data governance, data fiduciary duties, individuals' rights and the regulation of emerging technologies like AI, IoT and blockchain. It further considers whether these frameworks are adequate to meet the ethical and legal challenges posed by emerging technologies such as artificial intelligence, big data analytics and biometric surveillance.

4.2 EVOLUTION OF INTERNATIONAL DATA PROTECTION NORMS

The evolution of international data protection norms reflects the gradual yet profound shift in how societies perceive privacy in an increasingly digital and interconnected world. What began as a limited concern over administrative data misuse in a handful of industrialized nations has now transformed into a globally recognized legal and human rights imperative. Data protection has emerged not only as a technical or regulatory issue but as a central feature of democratic governance, human dignity, and transitional justice. The trajectory from early domestic legislation to internationally binding norms underscores a critical recognition of privacy as both an individual right and a collective interest in the digital economy. Data protection began to take shape in the 1970s as digital technology advanced and privacy concerns started to grow. Germany and Sweden were the first countries to introduce pioneering laws aimed at protecting personal information from misuse. The early effort laid the foundation for today's data privacy standards, influencing how societies around the world think about and regulate the handling of personal data. They marked a turning point in the legal response to digital transformation³²². This section explores the evolution in four pivotal phases: the initial legal response to data processing technologies in the mid-20th century, the grounding of privacy in universal human rights instruments, the

³²² *The Development of the Data Protection: From the GDPR to Global Standards*, Ailance 2B Advice, Jan 29, 2025, <https://2b-advice.com/en/2025/01/29/the-development-of-data-protection-from-the-gdpr-to-global-standards/#:~:text=The%20development%20of%20data%20protection%20has%20its%20roots%20in%20the,the%20misuse%20of%20personal%20data> (Last visited on June 01, 2025).

normative leap from soft law to binding international agreements, and finally, the complex legal terrain created by global digitalized and transborder data flows.

4.2.1 Early Developments

The first formal recognitions of data protection as a legal issue emerged in the 1960s – 1970s, driven by growing concerns about the use of mainframe computers in government and private sector data processing. Western democracies, particularly in Europe, have become increasingly wary of the ability of computerized systems to store, manipulate, and share vast quantities of personal information with minimal oversight. In 1970, the German state of Hesse enacted the world’s first data protection law, followed by Sweden’s landmark Data Act in 1973, which regulated personal data use by both public and private actors³²³. These pioneering efforts laid the groundwork for a broader European consciousness about the need to control information asymmetries between data subjects and processors. At the international level, the Council of Europe initiated discussions that would later culminate in Convention 108, the first legally binding treaty on data protection³²⁴. Although still nascent, this period was critical in establishing a vocabulary of rights and responsibilities around personal data. It was also characterized by a strong focus on administrative transparency, the prevention of authoritarian misuse of information, and the safeguarding of individual liberties in the face of growing surveillance capabilities. These early legal frameworks set the tone for future international efforts by emphasising consent, the legitimacy of processing, and the principle of purpose limitation, which still anchor contemporary data protection regimes.

³²³ Eur. Parl. Research Serv., *Understanding EU Data Protection Policy*, Briefing No. PE 698.898 (Jan. 2025), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI\(2022\)698898_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf).

³²⁴ Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, opened for signature Oct. 10, 2018, C.E.T.S. No. 223., <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> (Last visited on June 01, 2025).

4.2.2 Role of Human Rights Instruments

A foundational shift occurred when data protection began to be interpreted not merely as a regulatory tool, but as an extension of the fundamental human right to privacy. This evolution is anchored in key international human rights documents. Article 12³²⁵ of the Universal Declaration of Human Rights (1948)³²⁶ and Article 17³²⁷ of the International Covenant on Civil and Political Rights (1966)³²⁸ affirm the right of every individual to be protected against arbitrary interference with their privacy, family, home or correspondence. Although these instruments predate the digital era, their adaptability has enabled jurists and scholars to extend their interpretations into the realm of digital rights. The link between data protection and human dignity was further strengthened by regional courts, especially the European Court of Human Rights (ECHR) in the case of *Rotary v Romania*.³²⁹ The issue was raised as to whether the file containing information on the applicant's personal life was stored with the Romanian Intelligence Service, and was violating the Right to privacy under Article 8³³⁰ of the European Convention on Human Rights³³¹. The European Court of Human Rights found that Romania had violated his right to privacy under Article 8. The Court stressed that storing and using private data without proper legal safeguards or judicial oversight breached core democratic values.

³²⁵ G.A. Res. 217 A, Universal Declaration of Human Rights, art. 12- 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, (Dec. 10, 1948).

³²⁶ G.A. Res. 217 A, Universal Declaration of Human Rights, (Dec. 10, 1948) <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (Last visited on June 01, 2025).

³²⁷ International Covenant on Civil and Political Rights (1966) art-17 (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.

³²⁸ International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> (Last visited June 01, 2025)

³²⁹ *Rotary v Romania*, European Court of Human Rights, Application no 28341/95, 4th May 2000.

³³⁰ Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8- Right to respect for private and family life. 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of his rights except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or 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. Nov. 4, 1950, 213 U.N.T.S. 221.

³³¹ Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, https://www.echr.coe.int/documents/d/echr/convention_ENG (Last visited on June 03, 2025).

4.2.3 From Soft Law to Binding Instruments

The late 20th and early 21st centuries witnessed a significant normative transition from aspirational ‘soft law’³³² guidelines to enforceable international treaties and supranational regulations. Soft law, such as the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)*³³³, played a pivotal role in setting the stage for international consensus. These guidelines introduced essential principles such as collection limitations, purpose specification, data quality, and accountability. Although non-binding, they encouraged coherence in national laws and fostered trust in cross-border commercial data flows, especially among OECD member states. Yet the increasing ubiquity of digital platforms, coupled with high-profile data breaches and public distrust in tech companies, exposed the limitations of soft laws. The move toward binding instruments was spearheaded by the Council of Europe’s Convention 108, adopted in 1981, which remains the only international treaty dedicated exclusively to data protection. Its modernization in 2018 as *Convention 108+* reflects the evolving technological and geopolitical context, with enhanced protections for algorithmic decision-making, data portability, and international cooperation³³⁴. Perhaps the most transformative binding instrument to data is the *EU General Data Protection Regulation (GDPR)*, which came into effect in 2018. While a regional law, its extraterritorial application and stringent enforcement mechanisms have effectively globalized European data protection standards. Numerous countries have aligned aspects of their data protection laws with the GDPR to facilitate trade and ensure the adequacy of data transfers. This global regulatory

³³² The term soft law is used to denote agreements, principles and declarations that are not legally binding. Soft law instruments are predominantly found in the international sphere. UN General Assembly resolutions are an example of soft law. Hard law refers generally to legal obligations that are binding on the parties involved and which can be legally enforced before a court. European Centre for Constitutional and Human Rights, <https://www.ecchr.eu/en/glossary/hard-law-soft-law/#:~:text=The%20term%20soft%20law%20is%20used%20to,resolutions%20are%20an%20example%20of%20soft%20law.> (Last visited on June 03, 2025).

³³³ OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188, <https://legalinstruments.oecd.org/public/doc/114/114.en.pdf> (Last visited June 03, 2025).

³³⁴ Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *opened for signature* Oct. 10, 2018, C.E.T.S. No. 223., <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> (Last visited on June 03, 2025).

diffusion illustrates that binding instruments are not only legal tools but also a benchmark of technological ethics.

4.2.4 Digitalization and the Role of Transnational Data Flows

The fourth stage in the evolution of international data protection is characterized by the sheer scale, speed, and complexity of transnational data flows driven by digitalization. Unlike earlier phases, this era is characterized by real-time exchange of personal, biometric, behavioural, and transactional data across multiple jurisdictions, often through cloud infrastructure and AI-powered systems. The borderless nature of the internet and the global operations of data-driven corporations such as Google, Meta, Amazon, and Tencent have challenged the applicability of territorially bound legal systems. As data routinely crosses jurisdictions with differing or incompatible privacy standards, the risk of ‘*data dumping*’³³⁵ in lax regimes grows, undermining individual rights and regulatory coherence. International legal responses to this phenomenon have been piecemeal. Mechanisms such as Standard Contractual Clause, Binding Corporate Rules, and Adequacy Decisions have been developed to manage lawful cross-border data transfers. Regional initiatives, such as the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system, aim to ensure interpretability between privacy frameworks without enforcing regulatory uniformity. However, such instruments still operate within a fragmented global legal landscape. Apart from these global cases over the past two decades, a series of judicial decisions, regulatory interventions, and high-profile scandals have collectively contributed to the global awakening around the necessity of comprehensive data protection regimes.

The European Union has played a formative role, particularly through the Schrems I³³⁶ and Schrems II³³⁷ judgments of the Court of Justice of the European Union, which invalidated both the Safe Harbour and Privacy Shield frameworks,

³³⁵ Lynne, Pietro, Nik, Tom and Rebecca, Dictionary of Privacy, Data Protection and Information Security- Data Dumping- The practice of extracting data from a system and saving it to another system. It is usually used for data mining and backup. To avoid data breach, it is important to store data dumps in secure locations and limit the access to authorized users only, implementing access control, DOI: <https://doi.org/10.4337/9781035300921> (Last visited on June 03, 2025)

³³⁶ Maximillian Schrems v Data Protection Commissioner- C 362/14 (2015).

³³⁷ Data Protection Commissioner v Facebook Ireland Limited C-311/18 (2020).

citing inadequate safeguards against US surveillance practices. The Google Spain ruling further solidifies the EU's leadership by establishing the “*right to be forgotten*”, for grounding the individual's control over personal data in digital spaces. The Facebook Cambridge Analytica scandal exposed the vast vulnerabilities in data governance, as millions of users' profiles were harvested without consent for political manipulations³³⁸ an event that resonated far beyond regulatory circles and promoted urgent legislative reconsideration globally. Similar developments, such as Brazil's enactment of the LGPD, South Korea's ruling against Google's unauthorized location tracking³³⁹ and mounting security concerns over platforms like TikTok³⁴⁰ reflect a growing consensus across jurisdictions. These incidents, coupled with normative frameworks such as the United Nations resolution on privacy in the digital age, have underscored the pressing need for harmonized, rights-based, and enforceable international data protection standards.

Moreover, geopolitical tensions have further complicated matters. Differing philosophies between the “*European right-based model*”, the “*American sectoral models*” and the “*Chinese state-control models*” demonstrate the difficulties of achieving a truly global data protection regime. In this contested terrain, there is growing advocacy for data sovereignty, digital non-alignment, and multi-stakeholder governance frameworks that include civil society, the private sector, and technical experts. As data flows become central to international trade, development, security, and diplomacy, the future of data protection will depend on balancing innovation and efficiency with normative commitments to individual autonomy, transparency, and accountability. This phase in the evolution underscores the need for a transitional legal order for data, one that transcends state boundaries while respecting local values and constitutional identities.

³³⁸ Carole Cadwalladr and Emma Graham Harrison, *Revealed: 50 million Facebook Profiles harvested for Cambridge Analytica in major data breach*, The Guardian, Mar 17, 2018, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (Sat 17 Mar 2018, 22.03 GMT).

³³⁹ Sohn Ji-young, *Korea to investigate Google's covert location data collection*, The Korea Herald, Nov 23, 2017, 16:05:48, <https://www.koreaherald.com/article/1513674> (Last visited June 08, 2025).

³⁴⁰ Madison Minges, *National Security and the TikTok Ban*, American University, Jan 23, 2025, <https://www.american.edu/sis/news/20250123-national-security-and-the-tik-tok-ban.cfm#:~:text=The%20national%20security%20concerns%20surrounding%20TikTok%20stem%20primarily%20from%20its,to%20spread%20propaganda%20or%20disinformation.>

4.3 KEY INTERNATIONAL LEGAL INSTRUMENTS AND FRAMEWORKS

As the global dialogue on data protection matures, several international legal instruments have emerged as foundational pillars in shaping national legislation, guiding cross-border data flows, and influencing corporate compliance practices. While national laws reflect domestic priorities and cultural attitudes towards privacy, international frameworks provide the necessary scaffolding for regulatory convergence, particularly in the context of globalization and digital interdependence. While differing in their legal force, ranging from binding treaties to non-binding guidelines, these instruments share the common goals of protecting individual privacy while enabling responsible data use. This section examines four influential instruments: the Council of Europe's Convention 108+, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, the OECD Guidelines and the key United Nations Initiatives. Each framework reflects a unique legal philosophy and regional context, yet collectively, they contribute to the mosaic of international data governance.

4.3.1 Convention 108+

The Council of Europe's Convention 108³⁴¹, adopted in 1981, holds the distinction of being the first and only binding international treaty dedicated exclusively to data protection. Initially conceived to safeguard individuals against abuses arising from the automated processing of personal data, Convention 108 was a landmark in recognizing data protection as a transitional legal issue. Its historic significance lies in both its normative content and its inclusive nature, as it remains open to accession by non-European countries, thereby reinforcing its global ambition. With the rapid transformation of digital technologies and the emergence of new risks such as algorithmic profiling, cross-border surveillance, and biometric tracking, Convention

³⁴¹ Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *opened for signature* Oct. 10, 2018, C.E.T.S. No. 223., <https://rm.coe.int/1680078b37> (Last visited on June 03, 2025).

108 was modernized in 2018 into Convention 108+³⁴². This updated instrument integrated stronger accountability, obligations, enhanced transparency requirements and expanded rights for data subjects, such as the right to know the logic behind automated decisions and the right to object to data processing. Importantly, it introduces risk-based approaches to data governance, allowing flexibility while maintaining core protective standards. Convention 108+ also addresses the increasingly global nature of data transfers by advocating for compatible legal regimes and robust enforcement cooperation among data protection authorities. Its influences extend beyond Europe, with countries like Argentina, Tunisia, Morocco and Senegal aligning their national laws with its provisions³⁴³. Thus, Convention 108+ not only serves as a benchmark for European regulatory coherence but also as a vehicle for promoting global harmonization in data protection standards. Key Provisions of Convention 108+:

- **Article 5³⁴⁴- Legitimacy of Data Processing:** Personal data must be processed fairly and only for specific, explicit and legitimate purposes.
- **Article 6³⁴⁵- Special Categories of Data:** Introduces heightened protection for sensitive data, including biometric and genetic data.
- **Article 9³⁴⁶- Transparency and Rights of the Data Subjects:** Guarantees individuals the right to access their data, request rectifications, and object to processing.
- **Article 10³⁴⁷- Accountability:** Obligates data controllers to demonstrate compliance with the Convention's principles.

³⁴² Convention 108+ Convention for the protection of individuals with regard to the processing of personal data, Council of Europe, <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> (Last visited on June 03, 2025).

³⁴³ Handbook on European Data Protection Law, 2018 Edition, Council of Europe, https://www.echr.coe.int/documents/d/echr/Handbook_data_protection_ENG.

³⁴⁴ Convention for the Protection of Individuals with Regard to the Processing of Personal Data art. 5, Jan. 28, 1981, C.E.T.S. No. 108 (modernized 2018).

³⁴⁵ Convention for the Protection of Individuals with Regard to the Processing of Personal Data art. 6, Jan. 28, 1981, C.E.T.S. No. 108 (modernized 2018).

³⁴⁶ Convention for the Protection of Individuals with Regard to the Processing of Personal Data art. 9, Jan. 28, 1981, C.E.T.S. No. 108 (modernized 2018).

³⁴⁷ Convention for the Protection of Individuals with Regard to the Processing of Personal Data art. 10, Jan. 28, 1981, C.E.T.S. No. 108 (modernized 2018).

- **Article 14³⁴⁸- Cross-Border Data Transfer:** Permits international data transfer only when the receiving country ensures an equivalent level of protection.

Convention 108+ distinguished itself by integrating contemporary concepts such as privacy-by-design, risk-based regulation, and automated decision safeguards, anticipating challenges posed by artificial intelligence and algorithmic governance. It also mandates the establishment of independent supervisory authorities and encourages international corporations through a mutual assistance mechanism. By codifying both rights and obligations, Convention 108+ sets a high bar for balancing digital innovation with individual dignity.

4.3.2 APEC Privacy Frameworks

The Asia-Pacific Economic Cooperation (APEC) Privacy Framework, developed in 2005³⁴⁹ and updated in 2015,³⁵⁰ provides a non-binding but strategically significant approach to data protection within the dynamic and diverse economies of the Asia-Pacific region. This framework aligns closely with the foundational principles set out in the OECD's 1980 guidelines on the Protection of Privacy and Transborder Data Flows³⁵¹. Unlike the European model, which prioritizes individual rights and regulatory enforcement, the APEC framework adopts a business-friendly, trade facilitative approach that emphasizes interoperability over uniformity. At the core of APEC frameworks rest *nine key principles*³⁵², including preventing harm, notice, choice, collection limitation, use of personal information, integrity of personal information, security safeguards, access and correction, and accountability. These principles are designed to foster consumer trust and ensure the seamless flow of

³⁴⁸ Convention for the Protection of Individuals with Regard to the Processing of Personal Data art. 14, Jan. 28, 1981, C.E.T.S. No. 108 (modernized 2018).

³⁴⁹ Asia-Pacific Econ. Coop. [APEC], *APEC Privacy Framework*, December 2005, <https://www.apec.org/publications/2005/12/apec-privacy-framework> (Last visited on June 05, 2025).

³⁵⁰ Asia-Pacific Econ. Coop. [APEC], *APEC Privacy Framework*, (2017), [https://www.apec.org/publications/2017/08/apec-privacy-framework-\(2015\)](https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015)).

³⁵¹ OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/Legal/0188, (1980), <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188> (Last visited June 03, 2025).

³⁵² ASIA-PACIFIC ECONOMIC COOPERATION [APEC], *APEC PRIVACY FRAMEWORK* 12–25 (2005).

information across borders while allowing each member economy to implement context-sensitive privacy standards. The exceptions outlined in Part III of the framework include national sovereignty, national security, public safety and public policy³⁵³. A key innovation of the APEC framework in the Cross-Border Privacy Rules (CBPR) System³⁵⁴, which enables businesses to voluntarily certify their privacy practices with recognized accountability agents³⁵⁵. This system serves as a mechanism for ensuring baseline privacy protection in international data transfer without requiring formal legal harmonization among APEC members. As of now, economies like the United States, Japan, Canada, and Singapore participate in the CBPR system, with growing interest from others in the Asia Pacific region³⁵⁶. Despite its voluntary nature, the APEC Framework represents a pragmatic attempt to reconcile economic growth with data governance, especially in a region marked by regulatory diversity. It also offers a contrast to a more right-heavy framework, thereby enriching the global conversation on pluralistic approaches to privacy. The key provisions and Principles are:

1. **Preventing Harm**³⁵⁷: The core objective is to prevent misuse of personal information that could result in harm to individuals.
2. **Notice and Choice**³⁵⁸: Data subjects must be informed about the collection and use of their data and provided with meaningful choices.

³⁵³ Asia-Pacific Econ. Coop. [APEC], *APEC Privacy Framework*, ¶ 13 (2005) Exceptions to these Principles Contained in Part III of this framework, including those relating to national sovereignty, national security, public safety, public safety and public policy should be: (a) limited and proportional to meeting the objectives to which the exceptions relate; and (b) (i) limited and proportional to meeting the objectives to which the exceptions relate; and (ii) in accordance with law.

³⁵⁴ Asia-Pacific Econ. Coop. [APEC], *APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines* (Nov. 2019), <https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf> (Last visited on June 08, 2025).

³⁵⁵ APEC Cross-Border Privacy Rules System, CBPR Element 3-Recognition – para 22.

³⁵⁶ Steve Wood, *Global Cross-Border Privacy Rules and the new initiatives to support data free flow with trust*, A & O Shearman, July 19, 2023, <https://www.aoshearman.com/en/insights/ao-shearman-on-data/global-cross-border-privacy-rules-and-the-new-initiatives-to-support-data-free-flow-with-trust> (Last visited on June 08, 2025).

³⁵⁷ Asia-Pacific Econ. Coop. [APEC], *APEC Privacy Framework*, (2005). Principle I -Preventing Harm- Recognizing the interest of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

³⁵⁸ Asia-Pacific Econ. Coop. [APEC], *APEC Privacy Framework*, ¶¶ 15–17 (2005) Principle II- Notice.

3. Collection Limitations and Use Limitations³⁵⁹: Personal information should be collected by lawful and fair means and used only for the purposes stated at the time of collection.

4. Use of Personal Information³⁶⁰: Personal information collected should be used only to fulfil the purpose of collection.

5. Integrity and Security³⁶¹: Data must be accurate, complete and protected through reasonable security safeguards.

6. Access and Correction³⁶²: Individuals should have the right to access their data and request corrections when necessary.

7. Accountability Principles³⁶³: Organizations are responsible for complying with the framework and must take measures to protect data across the entire lifecycle, including when shared with third parties.

4.3.3 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

The OECD Guidelines, adopted in 1980³⁶⁴ and revised in 2013³⁶⁵, OECD Guidelines were among the earliest attempts to set international standards for privacy protection in the context of global trade. As a “soft law” instrument, the Guidelines are not legally binding on companies but carry considerable normative weight, especially among OECD member countries and partner economies³⁶⁶. They were developed in response

³⁵⁹ Asia-Pacific Econ. Coop. [APEC], APEC Privacy Framework, ¶ 18- (2005) Principle III.

³⁶⁰ Asia-Pacific Econ. Coop. [APEC], APEC Privacy Framework, ¶ 19- (2005) Principle IV.

³⁶¹ Asia-Pacific Econ. Coop. [APEC], APEC Privacy Framework, ¶ 22- (2005) Principle VII.

³⁶² Asia-Pacific Econ. Coop. [APEC], APEC Privacy Framework, ¶¶ 23-25- (2005) Principle VIII.

³⁶³ Asia-Pacific Econ. Coop. [APEC], APEC Privacy Framework, ¶ 26 (2005) Principle IX.

³⁶⁴ Org. for Econ. Co-operation & Dev. [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD/LEGAL/0188 (Sept. 23, 1980). <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188> (Last visited May 05, 2025).

³⁶⁵ Org. for Econ. Co-operation & Dev. [OECD], *The OECD Privacy Framework*, OECD/LEGAL/0188 (July 11, 2013), https://www.afapdp.org/wp-content/uploads/2018/06/oecd_privacy_framework.pdf.

³⁶⁶ Org. for Econ. Co-operation & Dev. [OECD], *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct* (2023) https://www.oecd.org/en/publications/oecd-guidelines-for-multinational-enterprises-on-responsible-business-conduct_81f92357-en.html (Last visited 5th June 2025).

to growing concerns about cross-border data flows and the lack of harmonized rules to protect privacy without stifling international commerce. The Guidelines articulate eight core privacy principles that have become foundational to many national laws: *collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability*. Moreover, by explicitly recognizing the legitimacy of transborder data flows under regulated conditions, the Guidelines provide a balanced framework that seeks to align privacy with economic development and innovation. Key Principles are:

- 1. Collection Limitation Principle:** Personal data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.³⁶⁷
- 2. Data Quality Principle:** Data should be relevant, accurate and kept up to date³⁶⁸.
- 3. Purpose Specification Principle:** The purpose for which data is collected should be specified at the time of collection³⁶⁹.
- 4. Use Limitation Principle:** Data should not be disclosed or used beyond the specified purpose without consent or legal authority³⁷⁰.
- 5. Security Safeguards Principles:** Reasonable protection should be in place against data loss, unauthorized access, or misuse³⁷¹.
- 6. Openness Principle:** Policies and practices regarding personal data should be transparent³⁷².

³⁶⁷ Org. for Econ. Co-operation & Dev. [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, ¶ 7, OECD/LEGAL/0188 (Sept. 23, 1980).

³⁶⁸ Org. for Econ. Co-operation & Dev. [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, ¶ 8, OECD/LEGAL/0188 (Sept. 23, 1980).

³⁶⁹ Org. for Econ. Co-operation & Dev. [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, ¶ -9, OECD/LEGAL/0188 (Sept. 23, 1980).

³⁷⁰ Org. for Econ. Co-operation & Dev. [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, ¶ 10, OECD/LEGAL/0188 (Sept. 23, 1980).

³⁷¹ Org. for Econ. Co-operation & Dev. [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, ¶ 11, OECD/LEGAL/0188 (Sept. 23, 1980).

³⁷² Org. for Econ. Co-operation & Dev. [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, ¶ 11- OECD/LEGAL/0188 (Sept. 23, 1980).

7. Individual Participation Principle: Individuals should have access to their personal data and be able to challenge its accuracy.³⁷³

8. Accountability Principle: The Data controller must be held accountable for complying with the above principles³⁷⁴.

In 2013 revisions, the Guidelines incorporated additional guidance on *risk management, breach notification*³⁷⁵ and *the role of privacy enforcement authorities*, reflecting the evolving complexity of digital environments. The OECD Guidelines have served as a blueprint for legislative development in both developed and emerging economies. Their influence is evident in the convergence of privacy norms across jurisdictions that otherwise differ significantly in legal traditions and cultural conceptions of privacy. Though voluntary, adherence to the OECD Guidelines is seen as a mark of legal maturity and global engagement, which has made them particularly attractive to countries seeking to build credibility in digital markets without adopting heavy-handed regulations.

4.3.4 United Nations Initiatives

The United Nations, as the primary multilateral body concerned with universal human rights and global cooperation, has engaged with data privacy primarily through its human rights apparatus and specialized agencies. While the UN has not produced a binding treaty dedicated solely to data protection, its initiatives play a critical role in shaping global discourse and moral expectations around digital rights. One of the earliest recognitions of privacy as a fundamental human right came through Articles 12 and 17 of the Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966)³⁷⁶. Building on these foundational texts,

³⁷³ Org. for Econ. Co-operation & Dev. [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, ¶ 13- OECD/LEGAL/0188 (Sept. 23, 1980).

³⁷⁴ Org. for Econ. Co-operation & Dev. [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, ¶ 14- OECD/LEGAL/0188 (Sept. 23, 1980).

³⁷⁵ The OECD Privacy Framework 2013- This provision covers both notice to an authority and notice to an individual affected by a security breach affecting personal data.

³⁷⁶ International Covenant on Civil and Political Rights, Dec. 16, 1966, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> (Last visited June 11, 2025).

the UN Human Rights Council and Office of the High Commissioner for Human Rights (OHCHR) have increasingly addressed data-related issues, particularly in the context of surveillance, artificial intelligence, and digital inequality. In 2013, after the Sweden revelations,³⁷⁷ the UN General Assembly adopted Resolution 68/167³⁷⁸ on ‘*The Right to Privacy in the Digital Age*’, which emphasized that the same rights people have offline must also be protected online³⁷⁹. Subsequent reports by the *Special Rapporteur on the Right to Privacy*³⁸⁰ have explored issues such as government surveillance, corporate data practices, and called for greater accountability, transparency, and International Intelligence Oversight mechanisms.

Moreover, agencies such as the United Nations Educational, Scientific and Cultural Organization (UNESCO) and United Nations Conference on Trade and Development (UNCTAD) have taken initiatives in areas like data ethics, digital trade and AI governance. For example, UNESCO’s *Recommendation on the Ethics of Artificial Intelligence*³⁸¹ (2021) was the first document on AI ethics. It applies to all 194 member states and includes principles that intersect with data protection, such as privacy, transparency, and fairness. It emphasizes human rights, transparency, inclusiveness, accountability, and sustainability. Key provisions include banning social scoring and mass surveillance³⁸², promoting fairness and non-discrimination³⁸³,

³⁷⁷ Edward Snowden: Leaks that exposed US spy Programme, BBC News, 17th January 2014, https://www.bbc.com/news/world-us-canada-23123964#:~:text=Edward%20Snowden:%20Leaks%20that%20exposed%20US%20spy,Latin%20America%20monitored%20*%20US%20spying%20errors (Last visited on 8th June 2025) and Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, The Guardian, 6th Jun 2013, <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> (Last visited June 06, 2025).

³⁷⁸ G.A. Res. 68/167, U.N. Doc. A/RES/68/167 (Dec. 18, 2013), (Last visited June 08, 2025)

³⁷⁹ G.A. Res. 68/167, *The Right To Privacy In The Digital Age*, ¶ 3- Affirms that the same rights that people have offline must also be protected online, including the right to privacy, U.N. Doc. A/RES/68/167 (Dec. 18, 2013).

³⁸⁰ Human Rights Council, *Report of the Special Rapporteur on the Right to Privacy*, U.N. Doc. A/HRC/40/63 (Oct. 16, 2019), <https://digitallibrary.un.org/record/3853352?ln=en&v=pdf>.

³⁸¹ U.N. Educ., Sci. & Cultural Org. [UNESCO], *Recommendation on the Ethics of Artificial Intelligence* (Nov. 23, 2021), <https://unesdoc.unesco.org/ark:/48223/pf0000381137> (Last visited June 11, 2025).

³⁸² U.N. Educ., Sci. & Cultural Org. [UNESCO], *Recommendation on the Ethics of Artificial Intelligence*, ¶ 26 (Nov. 23, 2021).

³⁸³ U.N. Educ., Sci. & Cultural Org. [UNESCO], *Recommendation on the Ethics of Artificial Intelligence*, ¶ 28, Principles- Fairness and non-discrimination, (Nov. 23, 2021).

and ensuring explainability of AI systems³⁸⁴. It also advocates for strong data governance, ethical impact assessments, and international cooperation, placing human dignity and social well-being at the heart of AI governance worldwide. The UNCTAD Technology and Innovation Report 2025, titled ‘*Inclusive Artificial Intelligence for Development*’³⁸⁵, emphasizes harnessing AI to reduce global inequality. It calls on policy to adopt science, technology, and innovation strategies that prioritize equity, digital inclusion and responsible AI governance. UNCTAD, in this report, advocates for an AI-for-all approach, addressing infrastructure, data and skills, to steer the technology towards shared goals and values. While UN instruments often lack enforcement teeth, their value lies in their ability to legitimize privacy as a global norm, facilitate multistakeholder dialogues, and frame data protection within a broader matrix of sustainable development, digital inclusion, and human rights.

4.4 REGIONAL APPROACHES TO DATA PROTECTION

As data is increasingly becoming the currency of the digital economy, countries around the world have adopted a distinct legal framework to regulate its collection, use, and transfer. While international treaties and guidelines set broad normative standards, the real-world enforcement, philosophical grounding, and practical operation of data protection laws often vary significantly at the regional and national levels. This section undertakes a comparative analysis of selected jurisdictions from each continent to assess how regional experience shapes, enriches, or challenges global data privacy norms. The countries selected for this study, namely the European Union (GDPR), California (North America), Canada (South America), South Africa (Africa), South Korea (Asia), and India’s neighbouring countries China have been chosen not merely for geographical representation but their unique legal posture and regulatory innovations. To understand a structured and in-depth understanding of these regimes, *ten key aspects were considered, which are:*

³⁸⁴ U.N. Educ., Sci. & Cultural Org. [UNESCO], *Recommendation on the Ethics of Artificial Intelligence*, ¶¶ 37, 38, 40- Principles -Transparency and Explainability, (Nov. 23, 2021).

³⁸⁵ UNCTAD, Technology and Innovation Report 2025, *Inclusive Artificial Intelligence for Development*, UN 2025, <https://unctad.org/publication/technology-and-innovation-report-2025> (Last visited June 08, 2025).

1. *Constitutional recognition of the right to privacy.*
2. *Enforcement Ecosystems.*
3. *Cross-Border Data Transfer Mechanism.*
4. *Surveillance, National Security and Intelligence Exceptions.*
5. *Algorithmic Transparency and Automated Decision-Making.*
6. *Intersection of DP Laws with Digital Trade and Innovation Ecosystems.*
7. *Algorithmic Governance and Emotional/Behavioural Data.*
8. *Data Fiduciary Obligations.*
9. *Right of the Data Principal.*
10. *Regulation of Emerging Technologies such as AI, IoT and blockchain.*

By applying these analytical dimensions across diverse jurisdictions, this section aims to present a holistic, comparative, and contextually grounded view of regional data protection regimes. It seeks to go beyond legislative texts to uncover the normative, structural, and operational realities that shape privacy in the global digital landscape.

4.4.1 EUROPEAN UNION: GENERAL DATA PROTECTION REGULATION 2018 (GDPR)

The European Union's General Data Protection Regulation³⁸⁶ (Hereinafter referred to as GDPR), enforced from May 25, 2018, is globally recognized as the most ambitious and rights-centric data protection law ever enacted. Born out of the EU's long-standing commitment to fundamental rights, particularly the right to privacy and data protection, the GDPR replaced the earlier Data Protection Directive 95/46/EC³⁸⁷, harmonizing legal standards across 27 Member States while offering unprecedented protection to individuals and unprecedented protections to individuals and

³⁸⁶ Regulation 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), 2016 O.J. (L 119) 1. <https://gdpr-info.eu/> (Last visited June 15, 2025).

³⁸⁷ Council Directive 95/46/EC 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, 1995 O.J. (L 281) 31, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046> (Last visited June 17, 2025).

unprecedented obligations to data controllers and processors³⁸⁸. Its extraterritorial reach, enforcement capabilities, and human rights foundation have not only transformed the EU's internal digital governance but have also influenced legislative reform globally. The GDPR stands apart due to its normative depth and operational sophistication. It is not merely a compliance framework; it is a constitutional expression of Europe's social-legal vision of data dignity, digital sovereignty, and accountability. The GDPR reflects the EU's deep commitment to human dignity, autonomy and informational self-determination, values enshrined in the Charter of Fundamental Rights of the European Union 2000³⁸⁹. The philosophical underpinning of the GDPR is informational self-determination, and this is reflected in its emphasis on transparency, purpose limitation, and consent as the default legal basis for data processing.

At its core, the GDPR is rooted in Articles 7³⁹⁰ and 8³⁹¹ of the Charter of Fundamental Rights of the European Union, which respectively protect the right to private life and the explicit right to personal data protection. Unlike jurisdictions where privacy protection is seen as a reactive measure against harm, the EU views it as a proactive entitlement to control one's informational identity. The GDPR's enforcement regime is marked by a multi-level, decentralized, yet coordinated institutional structure. Each member state has an Independent Supervisory Authority, and these are collectively governed by the European Data Protection Board (EDPB) under Article 68³⁹². The 'one-stop shop' mechanism allows for centralized handling of cross-border data issues, thereby minimizing regulatory fragmentation. Articles

³⁸⁸ The History of the General Data Protection Regulation, European Data Protection Supervisor, https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (Last visited June 17, 2025).

³⁸⁹ Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1, https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

³⁹⁰ Charter of Fundamental Rights of the European Union art. 7- Respect for private and family life- Everyone has the right to respect for his or her private and family life, home and communications, (2000) O.J. (C 364) 1.

³⁹¹ Charter of Fundamental Rights of the European Union, 2000/C 364/01, Art 8- 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 accessing 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.

³⁹² GDPR, *supra* note 386, art. 68.

58³⁹³ and 83 grant the Supervisory Authority significant investigative, corrective, and punitive powers. The law authorizes an administrative fine of up to € 20 million or 4% of a company's annual global turnover, making non-compliance a high-risk business decision. Landmark fines against Amazon, €746 million,³⁹⁴ Meta €1.2 billion³⁹⁵ and British Airways³⁹⁶ underscore the regulation's teeth. Enforcement also includes the power to suspend processing, issue a warning and mandate corrective measures.

Chapter 5³⁹⁷ of the GDPR establishes a robust framework to ensure that data transferred outside the EU retains its high level of protection. The Schrems I and II decisions by the CJEU invalidated the US-EU Safe Harbour and Privacy Shield frameworks, stressing that foreign surveillance laws must not undermine EU fundamental rights. This has catalyzed global reform, as non-EU countries must now align with GDPR standards to ensure seamless data flows. Cross-border data transfers are permitted only when:

³⁹³ GDPR, *supra* note 386, art. 58- (1) Each supervisory authority shall have all of the following investigative powers (2) Each supervisory authority shall have corrective powers (3) Each supervisory authority shall have authorization and advisory powers (4) The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter. (5) Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

³⁹⁴ The Administrative Court Confirms the Decision of the July 15, 2021, of the National Data Protection Commission to impose fine of 746,000,000 Euros on Amazon Europe Core SARL, As well as Corrective measures under penalty of a Daily Penalty of 746,000 Euros, Luxembourg, 19th March 2025, <https://justice.public.lu/fr/actualites/2025/03/tribunal-administratif-jugement-amazon-amende-cnpd.html>, and also [https://syrenis.com/resources/blog/luxembourg-amazon-fine/#:~:text=Luxembourg%20upholds%20%E2%82%AC746m%20Amazon%20fine%20*%20Luxembourg's,under%20the%20General%20Data%20Protection%20Regulation%20\(GDPR\).](https://syrenis.com/resources/blog/luxembourg-amazon-fine/#:~:text=Luxembourg%20upholds%20%E2%82%AC746m%20Amazon%20fine%20*%20Luxembourg's,under%20the%20General%20Data%20Protection%20Regulation%20(GDPR).)

³⁹⁵ 1.2 billion euro fine for Facebook as a result of EDPB binding decision, European Data Protection Board, 22nd May 2023, https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en (Last visited June 21, 2025).

³⁹⁶ IOC statement: Intention to fine British Airways £ 183.39m under GDPR for data breach, European Data Protection Board, 8th July 2019, https://www.edpb.europa.eu/news/national-news/2019/ico-statement-intention-fine-british-airways-ps18339m-under-gdpr-data_en#:~:text=Following%20an%20extensive%20investigation%20the,to%20protect%20fundamental%20privacy%20rights.%E2%80%9D and IOC fines British Airways £20m for data breach affecting more than 400,00 customers, GDPR Register, <https://www.gdprregister.eu/news/british-airways-fine/> (Last visited June 22, 2025).

³⁹⁷ Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU), Chapter 5- Transfer of Personal data to third countries or international organisations.

- The third country receives an adequacy decision (Article 45)³⁹⁸
- Transfers are protected through Standard Contractual Clause (SCCs) or Binding Corporate Rules (BCRs) (Article 46-47)
- Derogations under specific circumstances apply (Article 49), such as explicit informed consent.

While the GDPR allows certain exceptions under Article 23 for national security, defense, or public interest, these are narrowly interpreted and subject to proportionality and necessity principles. Importantly, such exceptions do not provide blanket immunity for state surveillance. The CJEU and European Court of Human Rights have invalidated several national laws that allowed indiscriminate mass data retention in the case of *Digital Rights Ireland*³⁹⁹, *Tele2 Sverige*⁴⁰⁰ *La Quadrature du Net*⁴⁰¹ and *Ministerio Fiscal*⁴⁰². These rulings of the Court of Justice of the European Union (CJEU) clarified the limits of state surveillance and data retention within the EU. The court declared the Data Retention Directive invalid, citing disproportionate interference with the fundamental right to privacy and data protection under the EU Charter. It further held that any national legislation allowing access to electronic communication data must be strictly necessary, proportionate and grounded in clear legal safeguards, especially when invoked on national security grounds⁴⁰³. The EU's approach is thus unique in its constitutional constraint on state power, insisting that even national security surveillance must respect core privacy guarantees.

The most forward-looking aspects of the GDPR is its regulation of automated decision-making and profiling. Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling that produces legal or similarly significant effects. While GDPR does not ban AI or profiling, it mandates

³⁹⁸ GDPR, supra note 386, art.45- Transfer 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 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.

³⁹⁹ *Digital Right Ireland Ltd v Minister for Communications, Marine and Natural Resources*, C-293/12 (2014).

⁴⁰⁰ *Tele2 Sverige AB v Post-och telestyrelsen*, C-203/15 (2016).

⁴⁰¹ *La Quadrature du Net* C-470/21 (2024).

⁴⁰² *Ministerio Fiscal* C-207/16 (2016).

⁴⁰³ Court of Justice of the European Union, Press Release No. 123/20, Luxembourg, 6th October 2020, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf>.

transparency, meaningful human intervention⁴⁰⁴, and right to explanation⁴⁰⁵ principles that have laid the groundwork for the proposed AI Act of the EU. Data subjects have the rights: (1) not to be subject to decisions made solely on automated processing, where such decisions produce legal or similarly significant effects, and (2) to demand meaningful information about the logic involved, as well as the significance and consequences of such processing.

Articles 13-15⁴⁰⁶ and 22⁴⁰⁷ of the GDPR introduce powerful rights concerning automated decision-making and profiling. Though often mischaracterized as a blanket ban, Article 22 mandates explicit consent or legal necessity for such processing, and insists on human oversight in critical decisions. These provisions are the legal foundation for Europe's emerging AI governance, including the forthcoming EU AI Act. The GDPR's global influence stems not only from its legal strength but also from its role in shaping data-enabled economic models. The '*privacy by design and by default*' principle compels developers and platforms to embed privacy into their system architecture (Article 25⁴⁰⁸). The regulation fosters trust in digital services,

⁴⁰⁴ Regulation 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) art. 22, 2016 O.J. (L 119) 1.

⁴⁰⁵ Id, Recital 71.

⁴⁰⁶ GDPR, supra note 386, art.13- Information to be provided where personal data are collected from the data subject. Art 14- Information to be provided where personal data have not been obtained from the data subject. Art 15- Right to access by the data subjects

⁴⁰⁷ GDPR, supra note 386, at art. 22- 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 authorized 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 right and freedom 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.

⁴⁰⁸ GDPR, supra note 386, art.25 Data Protection by design and by default- 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of determination of the means for processing and at the time of the processing and at the time of processing itself implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data protection principles, such as data minimization, in an effective manner and to requirements of this Regulation and protect the rights of data subjects.

promoting innovation through the use of privacy-preserving technologies such as pseudonymization, anonymization, and data minimization. The GDPR's synergy with the *EU Data Governance Act*⁴⁰⁹, *Digital Service Act*⁴¹⁰, and the *Digital Market Act*⁴¹¹ makes it a central piece of Europe's border digital sovereignty agenda. For Algorithmic data governance, while not explicitly naming emotion AI or neurodata, the GDPR's broad definitions of personal data (Article 4) and special category data (Article 9) extend to biometric, genetic, and inferred data. Behavioural profiling (e.g. online tracking, ad personalization) is heavily regulated under Recital 71⁴¹², which calls for protection against the discriminatory effects of profiling. The law thus anticipates the growing influence of affective computing and psychological targeting, offering a legal framework to limit its harm. In sectors like insurance, employment, and credit scoring, profiling practices must undergo Data Protection Impact Assessments (DPIAs) under Article 35⁴¹³.

⁴⁰⁹ European Data Governance and amending Regulation (EU) 2028/1724 (Data Governance Act) , Regulation (EU) 2022/868 of the European Parliament and of the Council, 30th May 2022, <https://eur-lex.europa.eu/eli/reg/2022/868/oj> (Last visited June 12, 2025).

⁴¹⁰ Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) , Regulation (EU) 2022/2065 of the European Parliament and of the Council, 19th October 2022, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065> (Last visited June 12, 2025).

⁴¹¹ Contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), Regulation (EU) 2022/1925 of the European Parliament and of the Council, dated 14th September 2022, <https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng> (Last visited June 15, 2025).

⁴¹² European Union, General Data Protection Regulation (GDPR) Regulation (EU) 2016/679, Recital 71- Profiling – The data subject have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes profiling that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

⁴¹³ GDPR, supra note 386, art 35- Data Protection Impact Assessment -1 Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Article 5 (Principles)⁴¹⁴ Article 24⁴¹⁵ and Recital 74 (Responsibility and liability of the Controller)⁴¹⁶, Recital 75 (Risks to the Rights and Freedoms of Natural Person)⁴¹⁷, Recital 76 (Risk Assessment)⁴¹⁸, and Recital 77 (Risk Assessment Guidelines). Accountability requires that the organization:

- Uphold purpose limitation and data minimization
- Ensure lawfulness and fairness of processing
- Document and demonstrate compliance

Although the term ‘fiduciary’ is not used explicitly, the GDPR envisions controllers as trustees of personal data, especially through duties like appointing Data Protection Officers (Article 37) and conducting risk assessments. The Right of the Data Principal under the GDPR codifies the most comprehensive catalogue of data subject rights, including:

1. Right to access (Article 15)⁴¹⁹: Individuals have the right to ask whether their personal data is being processed by a data controller. If processing is confirmed, they

⁴¹⁴ GDPR, supra note 386, at art 5- 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 purpose and not further processed in a manner that is incompatible with those purposes; (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization) (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 longer than is necessary for the purposes for which the personal data are processed; (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality)

⁴¹⁵ GDPR, supra note 386, art 24- Responsibility of the Controller- 1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and able to demonstrate that processing is performed in accordance with this Regulation.

⁴¹⁶ GDPR, supra note 386, at Recital 74 emphasizes the responsibility and liability of the controller- the data controller must be accountable for any personal data processing they conduct or delegate. They are expected to implement effective safeguards and show compliance with the GDPR.

⁴¹⁷ GDPR, supra note 386, at Recital 75 highlights that processing personal data can pose serious risks ranging from discrimination and identity theft to loss of rights or reputation, especially when sensitive information or large datasets are involved. It stresses the highest concern of profiling, vulnerable individuals like children, and any misuse that may limit personal freedom or control.

⁴¹⁸ GDPR, supra note 386, at Recital 76 emphasizes that to understand how data processing might affect someone’s right, we must consider what data is being used, how much, why, and in what context and the level of risk, whether low or high, should be judged.

⁴¹⁹ GDPR, supra note 386, art.15.

can request access to the specific personal data held about them. They have the right to know

- 1) Why their data is being processed (i.e., purpose behind the processing)
- 2) What kind of personal data is being handled?
- 3) Who receives or will receive their data, especially if it's shared with entities outside the EU or with international organizations.
- 4) For how long will their data be kept?
- 5) Individuals must be informed about their rights to request correction, deletion, or restriction of how their data is used and their right to object.
- 6) How to file a complaint in case of a data breach.
- 7) If the personal data wasn't collected directly from the individual, they have the right to know where it came from.
- 8) If decisions are made automatically using their data, such as profiling, they have a right to understand how it works, why it's used, and what effects it may have on them.
- 9) If their data is transferred to a third country, individuals must be informed of what legal protections or safeguards are ensured under GDPR.

2. Right to rectification (Article 16)⁴²⁰: Individuals have the right to ask for their inaccurate personal data to be corrected. They can also request that incomplete information be completed.

3. Right to Erasure/Right to be forgotten (Article 17)⁴²¹: Under Article 17, individuals have the right to request that their data be deleted without undue delay and organizations (data controllers) must do this promptly when one of the following applies:

⁴²⁰ GDPR, supra note 386, art. 16.

⁴²¹ GDPR, supra note 386, art. 17.

- 1) Data is no longer needed
- 2) The person withdraws their consent, and there is no other valid legal basis to continue processing their data.
- 3) The individual objects to the processing – Under Article 21(1), general objection and no overriding legitimate reason to continue processing; or Under Article 21(2), direct marketing and their objection must be respected without exception
- 4) Unlawful processing
- 5) The Controller is legally obliged under the law to delete the data.
- 6) The personal data was collected from a child in relation to offering online services, as described in Article 8(1).

4. Right to restriction of processing (Article 18)⁴²²: Under Article 18, individuals have the right to request that an organization limit the use of their personal data, meaning the data can still be stored but not actively used, under the following circumstances:

- 1) If the accuracy of the data is challenged by the data subject, in that case, its processing will be paused while the organization checks and confirms its correctness.
- 2) If the data was processed unlawfully, and the person chooses not to have it erased.
- 3) Data is no longer needed by the Controller but needed by the data subject.
- 4) If the person has objected to the processing of their data under Article 21(1), they can request a restriction while it is being determined whether the organization's legitimate reason outweighs their own.

⁴²² GDPR, supra note 386, art. 18.

5. Right to data portability (Article 20)⁴²³: Individuals have the right to obtain a copy of their personal data that they have provided to a data controller, in a structured, widely used and machine-readable format. This ensures the data can be easily reused or transferred across digital platforms. These rights apply when the data processing is based on consent or a contract, and the data is being processed through automated systems (not manually).

6. Right to object (Article 21)⁴²⁴: The individual may object to the processing of their personal data at any time if it is based on public interest or legitimate interests, including related profiling. Upon the objection, processing must stop unless the controller proves a compelling legitimate ground that overrides the individual's rights or is necessary for legal claims. Individuals have an absolute right to object to their data being used for direct marketing, including related profiling. These rights are actionable through accessible redress mechanisms, and individuals can lodge complaints directly with the Supervisory Authorities or pursue judicial remedies. Transparency obligations under Articles 12-14 ensure that individuals are fully informed and able to exercise their rights meaningfully.

The Regulation of Emerging Technologies under the GDPR is tech-neutral and future-proof. It applies equally to data collected through IoT sensors, AI applications, or blockchain networks. While blockchain poses challenges to data erasure and minimization, EU regulators have issued guidance on '*off-chain*' solutions and '*zero-knowledge proofs*' to reconcile privacy with immutability⁴²⁵. Furthermore, the GDPR underpins the regulatory architecture of emerging EU proposals, such as:

- Artificial Intelligence Act 2024⁴²⁶ - Regulating high-risk AI applications

⁴²³ GDPR, supra note 386, art. 20.

⁴²⁴ GDPR, supra note 386, art. 21

⁴²⁵ Dr Michele Finck, Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data Protection law? European Parliamentary Research Service, European Union, July 2019, ISBN 978-92-846-5044-6 [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).

⁴²⁶ Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), 2024 O.J. (L 1689) 1., <https://ai-act-law.eu/> (Last visited June 10, 2025).

- ePrivacy Regulation- refining the confidentiality of communications.
- European Health Data Space (EHDC)⁴²⁷- enabling secure medical data sharing.

The GDPR is not just a statute; it is a constitutional declaration of Europe's commitment to digital human rights. Its strength lies in the integration of ethical principles, rigorous enforcement, and legal adaptability. By placing individuals at the center of digital ecosystems, demanding accountability from both state and corporations, and anticipating future technological risks, the GDPR serves as the gold standard for data protection globally.

4.4.2 NORTH AMERICA: CALIFORNIA- PRIVACY RIGHT ACT 2020

In the absence of a comprehensive federal data protection law in the United States, California has emerged as the frontrunner in data privacy regulation, positioning itself as the state-level vanguard of digital rights. The *California Privacy Rights Act 2020*⁴²⁸ (hereinafter referred to as CPRA), passed in November 2020 and effective from January 1, 2023, builds upon the earlier *California Consumer Privacy Act of 2018*⁴²⁹ (hereinafter referred to as CCPA) of 2018. While the CCPA was groundbreaking, the California Privacy Rights Act significantly strengthened the regulatory architecture, drawing California closer to global data protection benchmarks like the EU's GDPR. The CPRA represents a hybrid model blending consumer protection logic with limited rights-based frameworks, and attempting to reconcile strong economic incentives for data-driven innovation with increasing public concern over surveillance capitalism and algorithmic opacity.

⁴²⁷ European Health Data Space Regulations (EHDS), Public Health, European Commission, https://health.ec.europa.eu/chealth-digital-health-and-care/european-health-data-space-regulation-ehds_en (Last visited June 10, 2025).

⁴²⁸ *The California Privacy Right Act 2020*, THE CPRA, came into effect from 1st January 2023, <https://www.caprivacy.org/cpra-text/> (Last visited June 22, 2025).

⁴²⁹ California Consumer Privacy Act 2018, CAL. CIV CODE [1798.100- 1798.199.100], https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (Last visited June 17, 2025).

Unlike the EU's right-centric GDPR, the CPRA is anchored more in consumer protection philosophy than in fundamental rights. While Article 1, Section 1 of the California Constitution⁴³⁰ recognizes privacy as an inalienable right, the CPRA does not embed it as a fundamental constitutional entitlement. Instead, it treats personal data as a consumer asset, giving individuals control over how businesses collect, sell and use it. This framing results in a more transactional approach to privacy, focusing on notice, choice, and opt-outs rather than privacy as dignity or informational self-determination. Nevertheless, by granting enforceable rights and transparency obligations, the CPRA has elevated privacy from a contractual matter to a quasi-right-based consumer entitlement in the American context. The Enforcement Ecosystem under the CPRA's most important innovations is the creation of the California Privacy Protection Agency⁴³¹ (CCPA), a first-of-its-kind independent regulatory body in the U.S. dedicated solely to privacy enforcement. The CCPA is tasked with rulemaking, audits, and administrative enforcement, thus relieving the Attorney General of primary oversight responsibilities. Administrative fines can reach up to \$ 7,500⁴³² per intentional violation, with special provisions for violations involving minors. As a state law, the California Privacy Rights Act does not extend to federal surveillance activities, which are governed by legislation such as the Foreign Intelligence Surveillance Act of 1978 (FISA) or the Patriot Act of 2001.

For Cross-border data transfer unlike the GDPR's robust and codified data transfer regimes, the CPRA does not impose formal restrictions on cross-border data flows. CPRA has not adopted mechanisms equivalent to the Standard Contractual Clause. However, it implicitly addresses the issue through contractual obligations between businesses and third-party service providers or contractors. Under Section 1798.100(d), businesses must ensure that personal information shared with third

⁴³⁰ California Constitution, art 1, § 1 - All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. <https://leginfo.legislature.ca.gov/faces/codedisplayexpand.xhtml?tocCode=CONS>.

⁴³¹ The California Privacy Right Act 2020, §. 24- Establishment of Privacy Protection Agency.

⁴³² The California Privacy Right Act 2020, 1798.155. Administrative Enforcement (a) Any business, service provider, contractor, or other person that violates this title shall be liable for an administrative fine of not more than \$2,500 for each violation or \$7,500 for each intentional violation or violating involving the personal information of consumer.

parties is governed by agreements that restrict use to specific purposes, reflecting a ‘purpose limitation’⁴³³.

Algorithmic Transparency and Automated Decision-Making, the California Privacy Rights Act does not go as far as the GDPR in regulating automated decisions. Section 1798.185(a)(16)⁴³⁴ authorizes the development of regulations that strengthen consumer rights in relation to the profiling and automated decision-making technologies. This indicates a growing legislative intent to address algorithmic opacity and introduces requirements for meaningful information about the logic processing. The Act embodies a deliberate attempt to balance consumer data protection with the imperatives of sustaining a competitive and innovation-friendly digital economy. Notably, section 1798.140(d)⁴³⁵ narrows the definition of ‘business’ to entities that meet specific thresholds of annual gross revenue, volume of personal information processed, or business models based on data monetization. This approach is designed to minimize compliance burdens for small and medium-sized enterprises, thereby avoiding regulatory overreach. The CPRA further endorses a risk-based governance model, allowing flexibility in compliance mechanisms proportionate to the nature and

⁴³³ The California Privacy Right Act 2020, § 4. § 1798.100 (d) A business that collects a consumer’s personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor that: (1) specifies that the personal information is sold or disclosed by the business only for limited and specified purposes; (2) obligates the third party, service provider, or contractor to comply with applicable obligations under this title and obligates those persons to provide the same level of privacy protection as is required by this title; (3) grants the business rights to take reasonable and appropriate steps to help to ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business’s obligations under this title.

⁴³⁴ The California Privacy Right Act 2020, § 1798.185 (a) (16)- Issuing regulations governing access and opt-out rights with respect to businesses use of automated decision making technology, including profiling and requiring businesses response to access request to include meaningful information about the logic involved in those decision making processes, as well as a description of the likely outcome of the process with respect to the consumer.

⁴³⁵ The California Privacy Right Act 2020, § 1798.140 (d) Business means: (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers’ personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumer’s personal information, that does business in the State of California, and that satisfies one or more of the following thresholds: (A) As of January 1 of the calendar year, has annual gross revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of section 1798.185 (B) Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households. (C) Derives 50 percent or more of its annual revenues from selling or sharing consumers’ personal information.

scope of data processing activities (Section 1798.100(a)(3))⁴³⁶. This facilitates the development of scalable and adaptive data practices that support innovation. Additionally, the Act mandates enhanced corporate accountability and ethical data stewardship, particularly through the introduction of Data Protection Assessments (Section 1798.185(a)(15)(B))⁴³⁷ and the expanded authority of the California Privacy Protection Agency (Section 1798.199.40). These provisions collectively reflect a regulatory framework that supports responsible innovation while aligning with international digital trade norms and ethical data economy principles.

For Algorithmic Governance and Emotional/ Behavioural Data, the CPRA introduces a new category of ‘sensitive personal information’ under section 1798.140 (ae)⁴³⁸, which includes- Geolocation, Racial/ethnic origin, religious beliefs, Genetic and biometric data, sexual orientation, personal information collected and analyzed concerning a consumer’s health, sex life, or mental or physical condition. Consumers can limit the use and disclosure of such data through the ‘Limit Use’⁴³⁹ opt-out mechanism, an important control lever over emotional data manipulation. Although

⁴³⁶ The California Privacy Right Act 2020, § 1798.100 (a) (3)- The length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine such period, provided that a business shall not retain a consumer’s personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.

⁴³⁷ The California Privacy Right Act 2020, § 1798.185 (a) (15) Issuing regulations requiring businesses whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security, to: (B) Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing with the goal of restricting or prohibiting the processing if the risks privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.

⁴³⁸ The California Privacy Right Act 2020, § 1798.140 (ae) Sensitive Personal Information means: (1) Personal information that reveals: (A) A consumer’s social security, driver’s license, state identification card, or passport number (B) A consumer’s account log-in, financial account, debit card, or credit card number in combination with any required security or access code password, or credentials allowing access to an account. (C) A consumer’s precise geolocation (D) A consumer’s racial or ethnic origin, religious or philosophical beliefs or union membership.(E) The contents of a consumer’s mail, email, and text messages unless the business is the intended recipient of the communication (2) (A) the processing of biometric information for the purpose of uniquely identifying a consumer (B) Personal information collected and analyzed concerning a consumer’s health (c) Personal information collected and analyzed concerning a consumer’s sex life or sexual orientation.

⁴³⁹ The California Privacy Right Act 2020, § 1798.121- Consumer’s Right to Limit Use and Disclosure of Sensitive Personal Information.

the California Privacy Rights Act does not explicitly adopt the term “fiduciary”, it embeds several quasi-fiduciary duties within its regulatory framework, indicating a shift towards trust-based data stewardship. Businesses subject to the Act are expected to handle personal data with heightened responsibility and transparency, reflecting evolving expectations around data ethics and accountability. Key obligations include:

1. Data Minimization: Under section 1798.100(c)⁴⁴⁰ businesses are required to collect, use, retain, and share personal information only to the extent necessary and proportionate to the purposes for which it was collected. This principle aligns with the core fiduciary idea of limiting use to what is in the consumer’s best interest.

2. Purpose Limitation and Retention Transparency: Section 1798.100 (a) (2) and (3) mandates that businesses inform consumers before collection about the categories of personal information collected, the purposes for which it will be used, and the duration for which the data will be retained ⁴⁴¹

3. Security Safeguards: In line with Section 1798.100(e)⁴⁴² businesses must implement reasonable security procedures and practices to protect personal information from unauthorized access, destruction, use, modification, or disclosure, showing due care over digital assets entrusted by consumers.

⁴⁴⁰ The California Privacy Right Act 2020, § 1798.100 (c) A business’s collection, use, retention, and sharing of a consumer’s personal information shall be necessary and proportionate to achieve the purposes for which the personal information was collected, or processed, or for another disclosure purpose that is compatible with the context in which the personal information was collected and not further processed in a manner that is incompatible with those purposes.

⁴⁴¹ The California Privacy Right Act 2020, § 1798.100 (a)(2) If the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used and whether such information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected, without providing the consumer with notice consistent with this section. (3) The length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine such period, provided that a business shall not retain a consumer’s personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.

⁴⁴² The California Privacy Right Act 2020, § 1798.100 (e) A business that collects a consumer’s personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, disclosure in accordance with Section 1798.81.5

4. Prohibition of Dark Patterns: The CPRA explicitly prohibits the use of ‘*dark patterns*’ user interface designs that subvert or impair consumer autonomy through Section 1798.140(I)⁴⁴³, which defines valid consent as being freely given, specific, informed, and unambiguous, and not obtained through deceptive design.

The rights of the Data Principal under the California Privacy Rights Act (CPRA) significantly expand upon the rights framework introduced by the California Consumer Privacy Act (CCPA), reinforcing the principle of informational self-determination. It not only reaffirms key consumer rights but introduces new, enforceable entitlements that enhance individual control over personal data across the digital ecosystem. The CPRA provides the following core rights :

1. Right to know/Access: Under Section 1798.110(a) and 1798.130(a)(2), consumers have the right to request information about the categories and specific pieces of personal data collected about them, including the purposes of processing and third-party disclosure⁴⁴⁴.

2. Right to Delete: Retained from the CCPA and further clarified in Section 1798.105 (a)⁴⁴⁵ Individuals can request the deletion of personal information collected, subject to certain legal exceptions.

3. Right to Correct Inaccurate Data: A key enhancement introduced by the CPRA, Section 1798.106(a) establishes the right to request correction of inaccurate personal data maintained by a business.

⁴⁴³ The California Privacy Right Act 2020, § 1798.140 (I) “Dark Pattern” means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy decision making, or choice, as further defined by regulation.

⁴⁴⁴ Businesses must respond to a consumer’s verifiable request to access, correct, or delete personal information within 45 days. A one-time 45-day extension is allowed with notice. Responses must be free of charge and provided in a usable, portable format, either via the consumer’s account, mail or electronically. Businesses are generally required to provide information covering 12 months before receiving a consumer’s request. However, after regulations are adopted, consumers may request data beyond this period if collected after January 1, 2022, unless retrieving it is impossible or unreasonably difficult. The law does not require data retention beyond necessity.

⁴⁴⁵ The California Privacy Right Act 2020, § 1798.105 (a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

4. Right to Opt Out of Sale or Sharing: Section 1798.120(a) grants consumers the right to direct a business not to sell or share their personal data, with ‘sharing’ broadly defined to include use for cross-context behavioural advertising (Section 1798.140 (ad)).

5. Right to Limit Use and Disclose of Sensitive Personal Information: Introduced in Section 1798.121(a), consumers can restrict the use of sensitive personal data such as geolocation, racial, or ethnic origin, health information, or biometric data to that which is strictly necessary for the service provided.

6. Right to Data Portability: Under Section 1798.130(a)(3)(iii)⁴⁴⁶, individuals have the right to receive their personal data in a structured, machine-readable format, and where feasible, request its direct transmission to another entity. Crucially, these rights are enforceable not only against businesses but also extend to ‘*service providers*’ and ‘*contractors*’ as defined in Section 1798.140. This broader scope enhances the consistency and reach of consumer protection across the data supply chain. In addition, Section 1798.130(a)(1)(A) mandates that businesses provide accessible, user-friendly methods for submitting rights requests, such as webforms, toll-free numbers, or account interfaces embedding empowerment through design.

Although the California Privacy Rights Act 2020 does not include express provisions targeting specific technologies such as AI or blockchain, its technology-neutral language and evolving rulemaking mandate allow the CPPA to adapt its application to emerging innovations. As AI and IoT become embedded in consumer products, and as blockchain applications raise questions about immutability vs erasure rights, California’s approach allows contextual expansion through interpretative guidance. The creation of the CPPA as a dynamic body ensures that technology-specific guidelines will emerge as these sectors mature. Thus, the California Privacy

⁴⁴⁶ The California Privacy Right Act 2020, § 1798.130 (a)(3)(iii) Provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format, which also may be transmitted to another entity at the consumer request without hindrance. “Specific piece of information” do not include data generated to help ensure security and integrity or as prescribed by regulation. Personal information is not considered to have been disclosed by a business when a consumer instruct a business to transfer the consumer’s personal information from one business to another in the context of switching services.

Rights Act represents a significant evolution in the American data protection jurisprudence, one that moves from purely commercial regulation towards a more rights-anchored consumer framework.

4.2.3 SOUTH AMERICA: CANADA- PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT 2000

Canada's approach to data protection is founded on the bifurcated regulatory model, with separate legislation for the public sector and private sector. The *Privacy Act 1985*⁴⁴⁷ governs federal government institutions, while the *Personal Information Protection and Electronic Documents Act (PIPEDA) 2000*⁴⁴⁸ applies to private-sector organizations engaging in Commercial activities. In the two decades since its enactment, PIPEDA has positioned Canada as a jurisdiction with a balanced, business-friendly yet rights-aware approach to data protection, an approach that has earned it adequacy status under the EU's GDPR. However, as digital ecosystems have evolved, so have the challenges confronting PIPEDA. From AI-driven profiling to data localization debates, the statute is now under review through the proposed *Consumer Protection Act*⁴⁴⁹ (CPPA). Yet PIPEDA remains instructive as a living example of how voluntary accountability and corporate data stewardship can function within a constitutional democracy. The Personal Information Protection and Electronic Documents Act 2000 is not rights-based in the traditional sense; it does not derive directly from the Canadian Charter of Rights and Freedoms. However, its purpose clause (section 3) articulates a balanced philosophy

“is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, uses and disclosure of personal information in a manner that recognizes the right

⁴⁴⁷ Privacy Act, R.S.C. 1985, c. P-21 (Can.), (amended on 6th March 2025) <https://laws-lois.justice.gc.ca/eng/ACTS/P-21/index.html>, (Last visited July 15, 2025).

⁴⁴⁸ Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (Canada).

⁴⁴⁹ Bill C 27- An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, Current Status is at consideration in Committee in the House of Commons, <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading> (Last visited July 15, 2025).

to privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances”⁴⁵⁰.

This dual focus on individual privacy and commercial necessity reflects a unique approach rooted in constitutional moderation and administrative pragmatism. The Supreme Court of Canada has recognized information privacy as a protected interest under Section 8⁴⁵¹ of the Charter. The enforcement ecosystem under the Personal Information Protection and Electronic Documents Act 2000 is administered by the Office of the Privacy Commissioner of Canada. Under section 11, individuals may file complaints with the Commissioner regarding alleged violations, and the Commissioner is empowered to investigate, summon and enforce the appearance, receive and accept any evidence, investigate, audit, issue reports, and recommendations. However, the lack of order-making power and the absence of administrative monetary penalties have long been a source of criticism. Remedies under PIPEDA are indirect, requiring the Commissioner to refer unresolved complaints to the Federal Court under Section 14, which may then grant remedies, including damages.

The PIPEDA does not prohibit cross-border data flows. However, it imposes accountability obligations on organizations that outsource data processing abroad. According to Schedule 1, Principle 1- Accountability⁴⁵², organizations remain responsible for personal information transferred to third parties and must use contractual or other means to provide a comparable level of protection. The Personal Information Protection and Electronic Documents Act 2000 contains limited national

⁴⁵⁰ Personal Information Protection and Electronic Documents Act 2000, § 3 (Canada).

⁴⁵¹ The Canadian Charter of Rights and Freedoms, § 8- Everyone has the right to be secure against unreasonable search and seizure, <https://open.canada.ca/data/en/dataset/06d31e10-a2a8-4d53-9ff3-567714a0a9f3/resource/adf3e432-4076-435b-88fb-46f094bc1ac4>, (Last visited June 22, 2025).

⁴⁵² Personal Information Protection and Electronic Documents Act 2000, Schedule 1, Principle 4.1.3- An organization is responsible for personal information in its possession to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

security exceptions, mostly through section 7(3), which permits disclosure of personal information without consent:

- To comply with a subpoena, warrant, or court order (section 7(3)(c))⁴⁵³
- To a government institution for purposes of law enforcement or national security, under prescribed conditions (section 7(3)(d)).
- Organizations may also disclose personal data without consent if the information is required to respond to an emergency that threatens the life, health or security of an individual (Section 7(3)(e) or it is for the detection, prevention, or suppression of fraud or other unauthorized activities (Section 7(3)(d.1))⁴⁵⁴ under specific conditions.

However, these exceptions are not absolute; organizations must carefully assess requests to ensure legality. The Office of the Privacy Commissioner of Canada (OPC) has actively investigated collaborations between private firms and public agencies, particularly where private surveillance practices intersect with state functions. Nevertheless, PIPEDA does not provide direct oversight over state surveillance bodies, which remain under other federal laws. For algorithmic transparency and automated decision-making, PIPEDA does not currently explicitly regulate automated decision-making or profiling. However, under Section 6.1, consent must be meaningful, requiring organizations to explain the purposes for which data is collected, including any use in profiling or automated decisions. The OPC has issued guidelines⁴⁵⁵ emphasizing that individuals should be informed when decisions are made based on algorithmic processes, and have the right to know the rationale and

⁴⁵³ Personal Information Protection and Electronic Documents Act 2000, § 7(3)(c)- requires to comply with subpoena or warrant issued or an order made by a court, person, or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of record;

⁴⁵⁴ Personal Information Protection and Electronic Documents Act 2000, § 7(3)(d.1) made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a provinces that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation.

⁴⁵⁵ OPC, Principles for responsible, trustworthy and privacy-protective generative AI technologies, 7th December 2023, https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/ (Last visited June 12, 2025).

implications⁴⁵⁶. While not codified, this has led to the emergence of soft-law principles on algorithmic transparency in Canada. The proposed CPPA (Section 63(3)⁴⁵⁷ intended to formalize these duties by introducing a right to explanation of significant automated decisions, aligning with GDPR like standards. PIPEDA has been instrumental in Canada's positioning as a trust-based data economy. It offers legal certainty and regulatory flexibility to businesses, enabling innovation in sectors like fintech, e-commerce, AI and health tech. PIPEDA's purpose-based framework is outlined in Schedule 1, prioritize flexibility over prescriptive rules.

- Accountability (Clause 4.1)- organizations are responsible for personal information under their control, including when transferred to third parties.
- Identifying Purposes (Clause 4.2) and Limiting Collection (Clause 4.4) – data must be collected for legitimate purposes and only to the extent necessary.
- Openness (clause 4.8)- Organizations must be transparent in their privacy practices.

This model enables organizations to adapt privacy practices to specific technological contexts while remaining within the law's broader compliance boundaries. It allows businesses to implement sector-specific codes of practice, consistent with the law's flexible compliance strategy. The Personal Information Protection and Electronic Documents Act 2000 does not distinguish between types of personal data based on sensitivity (as GDPR does with special categories). However, Schedule 1, Principle 4.3 states that the reasonable expectations of the individual are relevant in determining the appropriate form of consent. The type of consent an organization must seek depends on both the situation and how sensitive the personal information is. While data like medical or income records are usually sensitive, context matters; what seems ordinary, like a magazine subscription, could be sensitive if linked to personal

⁴⁵⁶ OPC, Statement on Generative AI, Roundtable of G7 Data Protection and Privacy Authorities, June 21, 2023, https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2023/s-d_20230621_g7/ (Last visited June 17, 2025).

⁴⁵⁷ Bill C-27, House of Commons of Canada, Consumer Privacy Protection Act, § 63 (3) If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual that could have a significant impact on them, the organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision.

interests or beliefs⁴⁵⁸. PIPEDA has, although not explicitly provided anything related to emotional or behavioural inferences drawn from online tracking, biometric data are considered sensitive, and typically require express and informed consent. However, the proposed Artificial Intelligence and Data Act (AIDA), which is part III of Bill C-27, is Canada's first attempt at creating a horizontal, risk-based regulatory framework on artificial intelligence. Although PIPEDA does not use the term data fiduciary, however, PIPEDA implicitly imposes fiduciary-like responsibilities on organizations through the "*Accountability Principles*" (Schedule 1, Principle 1), which includes obligations to:

1. Organizations are expected to act responsibly and transparently when handling people's personal information. If an organization collects or uses personal data, it is accountable for protecting it.
2. Assigning Responsibility (Principle 1 (4.1.1): An organization must formally designate someone to be in charge of privacy compliance. This person or team is responsible for ensuring that the company follows all the rules laid out in PIPEDA.
3. Third-party accountability (Principle 1 (4.1.3): If the organisation shares personal information with another company (e.g. for processing or storage), it doesn't lose responsibility. It must ensure that the third party protects the information at a comparable level through contracts or similar agreements.
4. Privacy at Practice (Principle 1 (4.1.4): Organizations must put their privacy commitment into action through
 - Clear internal procedures to protect data
 - A system for responding to complaints or inquiries
 - Training staff on their privacy roles and responsibilities.

⁴⁵⁸ Personal Information Protection and Electronic Documents Act 2000, Schedule 1, Principle 4.3.4- The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

- Easy-to-understand privacy policies that explain how personal information is handled.

Unlike GDPR, PIPEDA does not provide an express right to erasure, data portability or objection to processing to the Data Principal. The Office of the Privacy Commissioner has acknowledged the gaps and recommended their inclusion in future legislation. PIPEDA grants individuals the right to

1. Right to knowledge and Purpose Specification (Principle 2):- Organizations must clearly explain why personal information is being collected, at or before the time of collection. This ensures that individuals are not kept in the dark about how their data is being used. (1) Individuals have the right to know the purpose for which data is collected, and (2) Any new purpose requires renewed consent, unless required by law, Principle 2 (4.2.4).

2. Right to Consent (Principles 3 & 4- Consent & Limiting Collection):- Individuals have the right to consent to the collection, use or disclosure of their personal information:

- Consent must be a clear understanding of what data is being collected and why (Principle 4.3 and OPC's Guidelines for obtaining meaningful consent⁴⁵⁹)
- The form of consent (express or implied) depends on the sensitivity and context of the data (Principle 4.3.6)
- An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.
- Organisations must not condition services on consent to unnecessary data processing.

3. Right to Access (Principle 9- individual Access (section 4.9)):- Individuals have the right to know whether an organization holds their personal data, how it's being used, and whom it has been disclosed to.

⁴⁵⁹ Office of the Privacy Commissioner of Canada, *Guidelines for obtaining meaningful consent*, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/ (Last visited June 17, 2025).

- *4.9.1 Right to Confirmation and Disclosure:* Upon request, an organization must confirm whether it holds a person's information. If the data includes sensitive data, the organization must also explain how the data has been used and from which third party they have received it.
- *4.9.3- Disclosure to third party:* When responding to an access request, the organization should list the specific third parties who received the individual data. If the exact details are not available, the organization must provide a list of parties who may have received it based on standard practices.

4. Right to Challenge Accuracy and Completeness (Principle 6):- Data subjects can request that incorrect or outdated information be corrected. This could mean correcting, deleting or adding to the data.

5. Right to Challenge Compliance (Principle 10):- Individuals have the right to file complaints with the organization's designated privacy officer if they believe their privacy rights have been violated. Organizations must have a process to receive, investigate and respond to such complaints, and if unresolved, individuals may escalate the matter to the Office of the Privacy Commissioner of Canada (OPC).

6. Right to Protection and Transparency (Principle 7 -Safeguards and Principle 8- Openness):- Individuals have the right to expect that their data will be protected with appropriate safeguards, particularly when sensitive information is involved. The organization must be transparent about how it handles personal information. This information should be shared in a way that's clear, accessible, and easy for the average person to understand.

While PIPEDA was not designed with emerging technologies in mind, its principles-based and technology-neutral framework allows it to apply to AI, IoT, and blockchain, though not without interpretative strain. In the Clearview AI investigation of 2021,⁴⁶⁰

⁴⁶⁰ Joint investigation of Clearview AI, Inc by the Office of the Privacy Commissioner of Canada the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, 2nd February 2021, <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>.

the OPC found that facial recognition scraped from social media without consent violated PIPEDA⁴⁶¹. On June 18th, 2025, the G7 Data Protection and Privacy Authorities Roundtable⁴⁶² held in Chelsea, Quebec, was addressed by Philippe Dufresne, Privacy Commissioner of Canada. The central theme of the G7 roundtable is “*Collective Action Today for a Trusted Tomorrow*”, which reflects the joint regulatory responses to complex data challenges. G7 Heads of State had issued a joint statement on AI, endorsing a human-centric model of AI governance. This includes commitment to Respect for privacy, transparency and accountability, and encourages AI adoption responsibly.

4.4.4 AFRICAN CONTINENT: SOUTH AFRICA- THE PROTECTION OF PERSONAL INFORMATION ACT 2013

The *Protection of Personal Information Act* (hereinafter referred to as POPIA) No. 4 of 2013⁴⁶³ is South Africa’s comprehensive data protection legislation, enacted to give effect to the constitutional right to privacy under Section 14⁴⁶⁴ of the Constitution of the Republic of South Africa, 1996. POPIA came into full effect on 1st July 2021. It aims to balance the protection of personal information with the right to access to information and the free flow of data in a digital economy. POPIA is explicitly grounded in section 14 of the South African Constitution, which guarantees the right to privacy, including the privacy of communication and personal information. The Preamble and Section 2 of the Act reaffirm this philosophical orientation by stating that the Act is intended to “.... *give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party*”⁴⁶⁵. The Act also acknowledge the need to harmonize privacy with other rights, such as access

⁴⁶¹ Violation of Principle 4.3 of Schedule 1 as well as § 6.1 of the PIPEDA. Subsection 5(3) of PIPEDA.

⁴⁶² Opening remarks by the Privacy Commissioner of Canada at the G7 Data Protection and Privacy Authorities Roundtable, Office of the Privacy Commissioner of Canada, June 18, 2025, https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2025/sp-d-g7_20250618/ (Last visited June 19, 2025).

⁴⁶³ Protection of Personal Information Act, 2013 (No. 4 of 2013) Republic of South Africa.

⁴⁶⁴ Constitution of the Republic of South Africa, 1996, § 14- Privacy- Everyone has the right to privacy, which includes the right not to have (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communication infringed.

⁴⁶⁵ Protection of Personal Information Act, 2013 § 2(1) Purpose of the Act (S. Afr.).

to information and freedom of expression⁴⁶⁶. For effective enforcement, POPIA establishes the Information Regulator, an independent statutory body with a broad mandate, under Chapter 5 (sections 39-53). The Regulator has the powers to: (i) monitor and enforce compliance (section 40) and (ii) conduct an investigation and issue a compliance notice (section 90). POPIA includes both administrative and criminal sanctions. Violations of processing principles or non-compliance with enforcement notices can attract penalties up to R10 million or imprisonment of up to 10 years under sections 107⁴⁶⁷ and 109⁴⁶⁸. Cross-Border Data Transfer Mechanisms under POPIA place clear restrictions on cross-border data transfer under section 72. POPIA ensures that cross-border data transfers only happen when the recipient offers privacy protections that match South African Standards. A business or organization in South Africa (called “*responsible party*”) generally cannot send someone’s personal information to another country unless one of the following conditions is satisfied:

i. Adequate Protection in the Foreign Country: The overseas recipient must be subject to (i) a similar law, or (ii) Binding Corporate Rules, or (iii) A formal agreement. That ensures the data is handled in a way that respects the same core privacy standards as POPIA has.

ii. Consent from the Data Subject: If the person whose data is being transferred gives clear consent, the transfer is allowed.

iii. Necessary for a Contract with the Data Subject: If the transfer is needed to fulfil a contract with the individual (for example, to deliver a product or service), or to take steps they’ve asked for before a contract is signed, it’s permitted.

⁴⁶⁶ Protection of Personal Information Act, 4 of 2013, § 7(1) (S. Afr).

⁴⁶⁷ Protection of Personal Information Act 4 of 2013, §107 – Penalties. Any person convicted of an offence in term of this Act, is liable in the case of contravention of (a) section 100, 103(1), 104(2), 105(1), 106(1), (3) or (4) to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment;

⁴⁶⁸ Protection of Personal Information Act, 4 of 2013, § 109 (1) If a responsible party is alleged to have committed an offence in terms of this Act, the Regulator may cause to be delivered by hand to that person (hereinafter referred to as the infringer) an infringement notice which must contain the particulars contemplated in subsection (2). (2)(c) Specify the amount of the administrative fine payable, which amount may, subject to subsection (10), not exceeding R 10 million.

iv. Necessary for a third-party contract that benefits the data subject- If the transfer is required for a contract with another party (not the data subject), but it's clearly in the person's interest, it is allowed.

v. For the Benefit of the Data-Subject (without Consent): If the transfer is done for the person's benefit, and (i) it's not practical to get their consent and (ii) they would probably agree if asked, then the transfer can proceed.

The Protection of Personal Information Act applies to both the public and private sectors; it contains limited exemptions for national security and law enforcement. Section 6 provides that the Act does not apply to processing for National security, Defence, public safety, or state intelligence activities. Some situations are specifically excluded; this means the law does not apply in the following cases:

i. Personal or Household use

ii. Irreversibly De-identified Data: If personal information has been completely anonymized, meaning there's no way to trace it back to a specific individual, then it's not covered by POPIA. (Once data can't be re-identified, it's no longer personal information under the law)

iii. Public Bodies Handling National Security or Public Safety: POPIA does not apply to government bodies that are processing information for: National security, including identifying terrorist financing or related threats and Defense or public safety activities.

iv. Criminal Investigations and Law Enforcement Functions: The Act does not apply to data processing by public bodies if it is for:

- Preventing or investigating crime
- Identifying illegal money flows
- Prosecuting Offenders
- Executing sentences or legal sanctions. However, this exemption is only valid if other laws are in place to safeguard personal data in those specific contexts.

v. Cabinet and Provincial Executive Councils: The law does not apply to the Cabinet or the Executive Council of provinces when performing their official decision-making functions.

vi. Judicial Functions: POPIA does not interfere with courts and judges when they are carrying out their core judicial responsibilities.

Section 71 of the Protection of Personal Information Act is one of its most progressive provisions. It grants individuals the right not to be subject to a decision that is based solely on automated processing, including profiling, which significantly affects them.

i. General protection against Automated Decisions: People cannot be subject to a decision made only by an automated process if that decision has legal consequences or significantly impacts their life, such as decisions that assess or determine their job performance, creditworthiness, reliability, location, health, personal preferences and behaviour or conduct.

ii. Exceptions (when Automated decisions are allowed): Automated decision-making is permitted only under specific conditions, such as when:

(a) Contractual Processing- The decision relates to making or fulfilling a contract and either the person's request was fulfilled, or there are measures in place to protect their rights.

(b) Legal or Regulatory oversight: The decision is made according to a law or an approved industry code of conduct, and that law or code includes proper safeguards for protecting the person's interests.

iii. When automated decisions are allowed, the party responsible must provide extra protection, including

(a) Right to Respond: the person affected must be given a chance to question or challenge the automated decision, which is called making representations.

(b) Explanation of the Logic: The organization must explain how the system works, provide enough information about the logic behind the algorithm so that the person can understand how decisions were made.

The Protection of Personal Information Act 2013 recognizes that the free flow of information is vital to South Africa's economic growth, especially in an increasingly digital and globally connected economy. Its preamble explicitly commits to balancing the right to privacy and cross-border data flows. POPIA also allows for sector-specific codes of conduct under section 60, enabling industries to tailor compliance while still respecting core privacy rights. This flexibility fosters trust by design and supports responsible data innovation. For Algorithmic Governance and Emotional or Behavioural Data, POPIA does not use terms like emotional data or affective computing, but its definition of special personal information under section 26⁴⁶⁹ includes biometric data, philosophical beliefs, race or ethnic origin, trade union membership, health or sexual orientation. Processing such data is prohibited unless specific conditions under section 27 are met, such as consent, public interest, or legal obligation. This implicitly covers emotional profiling, especially when used for targeted advertising. The obligations of Data Fiduciary under POPIA- While the term data fiduciary is not used explicitly, POPIA introduces 8 key conditions for the processing of personal information, including:

- Condition 1- Accountability (Section 8)
- Condition 2- Processing Limitation (sections 9 to 12)
- Condition 3- Purpose specification (sections 13 and 14)
- Condition 4 – Further processing limitation (section 15)
- Condition 5 – Information quality (section 16)
- Condition 6 – Information Openness (sections 17 and 18)
- Condition 7 – Security safeguards (sections 19 to 22)
- Condition 8- Data subject participation (sections 23 to 25)

⁴⁶⁹ Protection of Personal Information Act 4 of 2013 §26- Prohibition on processing of special personal information (S. Afr).

i. Accountability (Section 8⁴⁷⁰): The party responsible must prove that all other conditions are being followed, much like a fiduciary must account for decisions made on someone else's behalf.

ii. Processing Limitation (Sections 9 to 12⁴⁷¹): Data must be collected fairly and lawfully and only with the data subject's consent or legal justification. Organizations must avoid excessive collection or usage of data for purposes that go beyond the original region. This reflects a commitment to data minimization and respect for individual autonomy.

iii. Purpose Specification (Section 13⁴⁷²): Personal information must be collected for a specific purpose, and steps must be taken to ensure that data subjects are aware of the purpose.

iv. Security safeguards (section 19- 22⁴⁷³): Organizations must implement appropriate technical and organizational measures to protect personal information from loss, unauthorized access by identifying risks.

The Act creates a rights-based framework that helps people understand, manage, and protect their personal data in a digital age where privacy risks are increasingly real and complex. The rights provided under the Act are

1. Right to Access Personal Information (Section 23⁴⁷⁴): Every individual has the right to ask whether an organization holds their personal data. The organization must provide this information within a reasonable amount of time at a reasonable cost and in a language that is easy to understand.

2. Right to correct and delete inaccurate information (section 24⁴⁷⁵): The data subject can request the correction and deletion of personal data. Under Section 14, deleted information is no longer permitted to be retained.

⁴⁷⁰ Protection of Personal Information Act 4 of 2013 § 8 (S. Afr.).

⁴⁷¹ Protection of Personal Information Act 4 of 2013 § 9-12 (S. Afr.).

⁴⁷² Protection of Personal Information Act 4 of 2013 § 13 (S. Afr.).

⁴⁷³ Protection of Personal Information Act 4 of 2013 § 19-22 (S. Afr.).

⁴⁷⁴ Protection of Personal Information Act 4 of 2013 § 23 (S. Afr.).

⁴⁷⁵ Protection of Personal Information Act 4 of 2013 § 24 (S. Afr.).

3. Right to Object to Processing (section 11 (3))⁴⁷⁶: A person can object at any time to the use of their personal information if it's being processed for reasons like protecting someone's interest or fulfilling an organization's interest, especially if they have a personal reason to disagree, unless a law specifically allows. Additionally, data subjects can object if their data is being used for direct marketing purposes.

4. Right to Lodge Complaints (section 74)⁴⁷⁷: Anyone who believes that someone's personal information has been mishandled or their privacy rights violated can file a complaint with the Information Regulator using the proper procedure. Additionally, if a person or organization disagrees with a decision made by an adjudicator under section 63(3), they can also raise a formal complaint with the Regulator.

5. Remedies under the Act⁴⁷⁸: Sections 99 to 106 collectively form POPIA's enforcement engine. They ensure that data protection rights are not just theoretical, but are legally enforceable through civil litigation and criminal sanctions.

(i) Civil Remedies (Section 99 – civil action for damages): This empowers data subjects to bring a civil claim against a responsible party for damages suffered due to a violation of POPIA, even if no intention or negligence is proven.

(ii) Criminal Offences and Penalties (sections 100- 106)- the Protection of Personal Information Act 2013 does not specifically mention technologies; its principle-based and sector-neutral drafting enables it to regulate AI, IoT, and even blockchain applications where personal data is involved.

⁴⁷⁶ Protection of Personal Information Act 4 of 2013 § 11 (3) (S. Afr.).

⁴⁷⁷ Protection of Personal Information Act 4 of 2013 § 74 (S. Afr.).

⁴⁷⁸ Protection of Personal Information Act 4 of 2013 § 99-106 (S. Afr.).

4.4.5: ASIA: SOUTH KOREA - PERSONAL INFORMATION PROTECTION ACT 2011

South Korea is widely recognized for having one of the most significant and comprehensive data protection regimes in Asia, primarily governed by the Personal Information Protection Act⁴⁷⁹ (Hereinafter referred to as PIPA) 2011, which has undergone major amendments in 2020 and 2023 to align more closely with international standards such as the GDPR. PIPA is notable for applying broadly to both public and private sectors, ensuring consistency in the protection of personal information across contexts. Rooted in South Korea's broader constitutional commitment to personal dignity and informational autonomy, PIPA has gained prominence for its robust enforcement architecture, granular consent requirements, and forward-looking provisions on emerging technologies. It stands out as a hybrid model, culturally sensitive yet globally interoperable, grounded in high standards of user rights, corporate accountability, and governmental transparency. South Korea's data protection philosophy is grounded in Article 17⁴⁸⁰ of its Constitution, which guarantees the right to privacy. PIPA functions as the statutory instrument giving effect to this constitutional right, articulating a strong ethos of informational self-determination. Article 1⁴⁸¹ of the Personal Information Protection Act outlines its purpose and positions privacy as a right, not merely a regulatory expectation, distinguishing South Korea's approach from more transactional models. The enforcement framework under PIPA is centralized yet multifaceted. The 2020 amendment strengthened the powers of the Personal Information Protection Commission (PIPC)⁴⁸², making it the primary and independent supervisory authority.

⁴⁷⁹ Personal Information Protection Act 2011, (No 10465), South Korea, 29th March 2011, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG, last amended by Act no. 19234 on 14th March 2023, (https://elaw.klri.re.kr/eng_service/lawView.do?lang=ENG&hseq=62389)

⁴⁸⁰ The Constitution of the Republic of Korea 1948, art 17- The privacy of no citizen shall be infringed.

⁴⁸¹ Personal Information Protection Act 2020, (Act no 16930) art 1- The purpose of this Act is to protect the freedom and rights of individuals, and further, to realize the dignity and value of the individuals, by prescribing the processing and protection of personal information. (Amended by Act No. 12504, March 24, 2014).

⁴⁸² Personal Information Protection Act 2020, (Act no 16930) art 7 Personal Information Protection Commission shall be established under the Prime Minister to independently conduct work relating to the protection of personal information.

Under Articles 7-9, the Personal Information Protection Commission is empowered to conduct privacy impact assessments (Article 33⁴⁸³). If a public institution handles personal information in a way that may pose privacy risks based on specific criteria set by the Presidential Decree, it must carry out a Privacy Impact Assessment (PIA). This involves analyzing potential risks and proposing improvements. The assessment must be conducted by an organization approved by the Protection Commission, and the final report must be submitted to the Commission for oversight. The establishment of the Master Plan to protect personal information and its implementation. Article 7-9⁴⁸⁴ deals with matters concerning the improvement of the policies, systems, and laws relating to personal information protection. Article 75⁴⁸⁵ of PIPA deals with matters concerning the enactments, amendments and abolition of law under their jurisdiction and rules of the Protection Commission and the imposition of administrative fines

Personal Information Protection Act 2020 strictly regulates international data transfer through Article 28-8⁴⁸⁶. As a general rule, personal information cannot be transferred overseas, whether by sharing, outsourcing, or remote storage, unless one of the several specific exceptions applies. Organizations may only transfer personal information overseas when:

- 1. Informed Consent:** The transfer is permitted if the individual has given separate and clear and after being fully informed.
- 2. Legal or International Requirements:** Transfers are allowed if they are required by other laws, treaties, or international agreements.
- 3. Contractual Necessity:** Transfers are allowed if they are needed to perform or conclude a contract with the individuals, as long as Implements strong security and data protection measures and ensure that certified privacy practices are properly followed in the recipient's country.

⁴⁸³ Personal Information Protection Act 2020, (Act no 16930) art 33, (S. Kor.).

⁴⁸⁴ Personal Information Protection Act 2020, (Act no 16930) art 7-9, (S. Kor.).

⁴⁸⁵ Personal Information Protection Act 2020, (Act no 16930) art 75, (S. Kor.).

⁴⁸⁶ Personal Information Protection Act 2020, (Act no 16930) art 28-8 Inserted by 2023 Amendment (Act no 19234) dated 14th March 2023.

4. Equivalent Protection in the Recipient Country: The Protection Commissioner can approve a transfer if the foreign country or international organization offers data protection, user rights and remedies that are comparable to the Korean Standard.

5. Compliance and Additional measures: The organizations must also follow all general PIPA obligations (including Articles 17-19⁴⁸⁷ and Chapter V). They must implement security measures and legal safeguards set out by Presidential Decree, and contracts for overseas data transfer cannot include terms that violate PIAP.

Article 28-8⁴⁸⁸ establishes a general principle that a personal information controller may not transfer personal information across borders, unless some specific conditions are fulfilled, which are well-defined. These exceptions encompass the data subject giving express consent, such transfer being authorized by the relevant laws, treaties or international agreements and where the transfer is required to perform a contract with the data subject, with reasonable notice being made through privacy policies or other stipulated methodologies of communication. There are also exceptions when transfers are allowed in instances where the recipient has acquired recognized certification to guarantee the proper data protection practices, or when the destination country or organization has the capability to provide the same degree of protection as the one guaranteed by the Act. In line with this, Article 28-9⁴⁸⁹ gives the Protection Commission the power to suspend transfers across borders when such transfers are against the law or a source of harm because of insufficient protection in the destination jurisdiction. Provisions for the Cross-border data transfer under the Personal Information Protection Act contain limited exemptions for national security and public safety under Article 58(1)⁴⁹⁰, which permits certain public institutions to process personal data without consent when necessary. Certain parts of PIPA do not

⁴⁸⁷ Personal Information Protection (Amended) Act 2023, (Act no 19234) art 17- Provisions of personal information, art 18- Restriction on Repurposing Personal information and Provisions thereof, art 19- Restriction on use and provision of personal information on the part of its recipients, (S. Kor.).

⁴⁸⁸ Personal Information Protection Act 2020, (Act no 16930) art 28-8, (S. Kor.).

⁴⁸⁹ Personal Information Protection Act 2020, (Act no 16930) art 28-9, (S. Kor.).

⁴⁹⁰ Personal Information Protection (Amended) Act 2023, (Act no 19234) art 58(1) Partial Exclusion from Application, (S. Kor.).

apply in specific situations where strict enforcement could interfere with national interests or fundamental rights like freedom of expression or association.

i. Some personal information is excluded from the main rule of PIPA (chapters III – VIII) when it is used for national security purposes and for public interest activities.

ii. Certain PIPA provisions (Article 15⁴⁹¹, 22⁴⁹², 22-2, 27(1)-(2)⁴⁹³, 34⁴⁹⁴, and 37⁴⁹⁵) do not apply to personal data collected through fixed video surveillance systems installed in public areas under Article 25(1).

iii. If an organization processed personal information to run a friendship-based group like a hobby club, then Articles 15, 30, and 31 (which involve consent and privacy policy) do not apply.

iv. Even when these exceptions apply, the organization must limit data collection and use only what's necessary. Keep the data only for as long as needed and ensure safety and responsible use of data through technical protection and grievance handling processes.

For Algorithmic Transparency and automated Decision-Making, the significant amendment of 2023 is Article 37(2) of the Personal Information Protection Act introduced a new right for data subjects to request an explanation when significant decisions are made based solely on an automated process. Under PIPA, algorithmic decision-making and behavioural data are not left unregulated, even though they are not called out as separate categories. Through a mix of rights-based provisions (Article 37-2), consent rules (Article 15) and pseudonymization safeguards (Article 28-2 to 28-5), PIPA acknowledge the risks posed by automated decision-making

⁴⁹¹ Personal Information Protection (Amended) Act 2023, (Act no 19234) art 15- Collection and Use of Personal Information, (S. Kor.).

⁴⁹² Personal Information Protection (Amended) Act 2023, (Act no 19234) art 22- Methods of obtaining consent and art 22-2 Protection of Children's Personal Information, (S. Kor.).

⁴⁹³ Personal Information Protection (Amended) Act 2023, (Act no 19234) art 27 – Restriction on Transfer of Personal Information following Business Transfer, (S. Kor.).

⁴⁹⁴ Personal Information Protection (Amended) Act 2023, (Act no 19234) art 34- Notification and Reporting of Divulgence of Persona; Information, (S. Kor.).

⁴⁹⁵ Personal Information Protection (Amended) Act 2023, (Act no 19234) art 37- Suspension of Processing of personal Information, (S. Kor.).

profiling context. Article 37-2 empowers individuals to object to automated decision-making:

- i. If a decision that significantly affects a person's right or obligations is made entirely by an automated system (including AI), the individual has the right to object to that decision.
- ii. If such automated decisions are made, the individual can ask the organization to explain how and why it was made.
- iii. When someone objects to the decision or requests an explanation, the organization must either:
 - Pause or cancel the automated decision unless it has a strong justification not to, or
 - Take appropriate action, such as reviewing the decision with human involvement or offering a proper explanation.
- iv. Organization must clearly disclose the criteria, process, and data-handling methods used in making automated decisions so that individuals can easily understand and verify how their data is being used.
- v. Details about how people can object, ask for an explanation, and how organizations should respond will be set out in the Presidential Decree. This includes specifics about procedures, disclosure rules, and when automated decisions may still be applied.

Thus, Article 37-2 gives individuals the right to challenge important decisions made solely by automated systems, including AI. It ensures that people can ask for human review, explanations, and greater transparency, making sure algorithmic decisions do not happen in a black box. South Korean data law is designed to enable responsible innovation. PIPA includes a "pseudonymized data" regime (Article 28-2 to 28-7) introduced in 2020, which allows for data to be used without consent if it is de-identified and used for statistical, scientific or research purposes. This article promotes data-driven innovation and research while still protecting individual privacy by ensuring the data cannot be easily traced back to a person.

i. Processing of Pseudonymized Information (Article 28-2⁴⁹⁶): The organizations are allowed to use pseudonymized personal information where identifying details are removed and while sharing data with others, under the rules requires that the organization must ensure that no information is included that could be used to re-identify a specific person.

ii. Limits on Combining Pseudonymized Data (Article 28-3⁴⁹⁷): Article 28-3 adds an extra layer of protection by limiting who can combine pseudonymized data across institutions, ensuring that even de-identified data is handled with care and oversight, especially when it's shared beyond the combining entity. If an organization wants to send the combined dataset outside the institution, it must re-pseudonymize the information. When using pseudonymized data under Article 28-2 or 28-3, organizations must apply strong safety measures like separately storing re-identification keys to prevent data breaches or misuse. They may set their own retention periods based on purpose and must keep detailed records for at least three years after the data is deleted.

The Personal Information Protection Act does not use the term fiduciary, but article 3 imposes duties on personal information controllers. Core principles for handling personal information are

i. Clear purpose & Minimal collection: Organizations must clearly state why they are collecting data only as much as needed to achieve that purpose.

ii. Purpose limited use: Personal information only for the stated reasons and in ways that are appropriate and necessary.

iii. Safe Management: Personal data must be securely managed with safety measures appropriate to the type of data and the risk of harm to individuals' rights.

iv. Transparency & Rights Protection: Organizations must publicly share their privacy policies and make it easy for individuals to access their personal data.

⁴⁹⁶ Personal Information Protection (Amended) Act 2023, (Act no 19234) art 28-2 (S. Kor.).

⁴⁹⁷ Personal Information Protection (Amended) Act 2023, (Act no 19234) art 28-3 (S. Kor.).

v. Privacy by Design: Data should be handled in ways that reduce privacy risks as much as possible from the outset.

vi. Prefer Anonymization or Pseudonymization: Organizations should prioritize the approach for data protection.

v. Duty to safeguard (Article 29⁴⁹⁸): All personal information controllers must implement technical, managerial, and physical safeguards like internal policies and access logs to protect data from loss, theft, leaks, tampering, or damage as required by regulation.

Personal Information Protection Act guarantees data subjects' rights under Articles 35-38; these rights are designed to be accessible, actionable, and responsive, with defined timelines and appeal mechanisms.

i. Right to Access Personal Information (Article 35⁴⁹⁹): Individuals have the right to request and view the personal information that an organization holds about them. However, an organization can deny or restrict access, but only in specific situations such as

- When a law explicitly prohibits or restricts access
- If giving access could harm someone's safety, property, or rights.
- If access seriously interferes with government functions.

ii. Right to request Transfer of Personal Information (Article 35-2): Article 35-2 introduces a data portability right, allowing individuals to receive or transfer their personal data to trusted entities in a structured, usable format. The data must be transferable in a computer-readable format that is practical, considering cost, time and technical feasibility. The individuals can transfer requests at any time.

iii. Apart from this, Article 4 of the PIPA ensures that individuals have key rights over their personal data, to be informed, to give or withhold consent, to access and transfer their data, to request correction or deletion, to seek compensation for harm, and to

⁴⁹⁸ Personal Information Protection (Amended) Act 2023, (Act no 19234) art 29 (S. Kor.).

⁴⁹⁹ Personal Information Protection (Amended) Act 2023, (Act no 19234) art 35 (S. Kor.).

object to or challenge fully automated decisions affecting them ensuring fairness and control in data use.

Lastly, South Korea's Personal Information Protection Act does not have direct provisions governing emerging technologies. However, the National Guidelines for AI Ethics 2020⁵⁰⁰ serves as a comprehensive ethical framework to guide all sectors. The framework is based on three interconnected layers: the highest value, humanity, three basic principles and ten key requirements safeguarding human rights. Protection of privacy, respect for diversity, prevention of harm, public-good orientation, solidarity, ethical data management, clear accountability, safety assurance, transparency, and explainability.

4.4.6 NEIGHBOURING COUNTRY: CHINA- PERSONAL INFORMATION PROTECTION LAW 2021

China's *Personal Information Protection Law 2021*⁵⁰¹ (hereinafter referred to as PIPL), enacted in August 2021 and effective from November 1, 2021, represents a watershed moment in the development of data protection law within an authoritarian regulatory state. As China's first comprehensive privacy statute, the PIPL draws conceptually from international norms like the EU's GDPR, yet is deeply influenced by national security imperatives, digital sovereignty doctrine, and the Party-state model of governance. Together with the *Cybersecurity Law* (2017)⁵⁰² and the *Data Security Law* (2021)⁵⁰³, the PIPL forms part of a tripartite regulatory framework that reflects the state's ambition to achieve technological dominance, information control, and economic modernization, while offering a framework for individual protection within the bounds of national policy. The PIPL adopts many rights-based features but does so within a legal system that subordinates individual liberties to collective interest and regime stability. China's Constitution recognizes privacy and dignity in

⁵⁰⁰ National Guidelines for AI Ethics, 23rd December 2020, Korea Information Society Development Institute, <https://ai.kisdi.re.kr/eng/main/contents.do?menuNo=500011> (Last visited June 17, 2025).

⁵⁰¹ Personal Information Protection Law 2021(PIPL) People's Republic of China (NPC) dated 20th August 2021, <https://personalinformationprotectionlaw.com/> (Last visited June 20, 2025).

⁵⁰² Cybersecurity Law of the People's Republic of China 2017.

⁵⁰³ Data Security Law of the People's Republic of China 2021 dated 10th June 2021.

broad terms (Article 38⁵⁰⁴), but lacks an explicit enforceable right to privacy. The PIPL in Article 1 states that its purpose is to “*protect personal information rights and interests, regulate the processing of personal information, and promote the reasonable use of personal information*”. This reflects a statist and instrumental approach. The law protects personal data not as an inalienable right but as a component of a harmonious digital order.

The Personal Information Protection Law grants primary enforcement power to the Cyberspace Administration of China (CAC), with auxiliary roles played by sector-specific regulators such as the Ministry of Industry and Information Technology (MIIT) and the State Administration for Market Regulation (SAMR)⁵⁰⁵. Articles 60-71 of the PIPL outline enforcement tools:

1. Article 63⁵⁰⁶ allows personal information protection authorities to investigate data practices by questioning involved parties, reviewing records and contracts, conducting on-site inspections, and, if approved, seizing illegal data processing equipment.
2. When authorities identify high-risk or security incidents in how personal data is handled, they can summon responsible officials for questioning or require an external compliance audit.
3. Under Article 66⁵⁰⁷, organizations found to violate data protection obligations may be subject to a range of administrative sanctions. Regulatory Authorities are empowered to order rectification, issue a warning, and suspend or terminate services. Where rectification is refused, the data processor may be subject to a fine of up to RMB 10,000,00 while a directly responsible individual may be liable to a fine from

⁵⁰⁴ Constitution of People’s Republic of China 1982, art 38- The personal dignity of citizens of the People’s Republic of China shall not be violated. It is prohibited to use any means to insult, libel or falsely accuse citizens,

⁵⁰⁵ Shreya, *China’s Personal Information Protection Law (PIPL)*, CookieYes, Jun 2, 2025, <https://www.cookieyes.com/blog/china-personal-information-protection-law-pipl/#:~:text=The%20Cyberspace%20Administration%20of%20China%20is%20the,Science%20and%20Technology%20to%20enforce%20the%20law.> (Last visited June 20, 2025).

⁵⁰⁶ Personal Information Protection Law 2021(PIPL) art 63 (China).

⁵⁰⁷ Personal Information Protection Law 2021(PIPL) art 66 (China).

RMB 10,000 to RMB 100,000. In case of a serious violation, the authority may impose a fine of up to RMB 50 million or 50% of the organization's annual turnover.

4. Article 40 of the PIPL provides that if a personal information processor unlawfully handles data in a manner that harms the rights and interests of a large number of individuals, then designated entities, including the People's Procuratorate, authorized consumer organizations, and entities approved by the State Cyberspace Administration, may initiate legal action.

Personal Information Protection Law China adopts a highly restrictive model for cross-border data transfers. Chapter III articles 38-43 mandate:

1. Article 38⁵⁰⁸ stipulates that personal data may only be transferred under specific legal conditions if the personal information processor:

- (i) Successfully pass a security assessment organized by the State Cyberspace Administration under Article 40.
- (ii) Obtain certification by a recognized institution in line with regulatory requirements.
- (iii) Enters into a standardized contract with the overseas recipient, as per the State Cyberspace Administration.
- (v) Fulfils other conditions outlined in applicable law, regulations and guidelines.

2. According to Article 39⁵⁰⁹, transferring personal information outside China, the processor must clearly inform the individuals about the recipient's identity, purpose, method of processing, data type involved, right enforcement mechanisms and must obtain the individual's explicit consent.

3. Article 40⁵¹⁰ mandates that critical information infrastructure operators and large-scale personal data processors must store data collected within China. Cross-border

⁵⁰⁸ Personal Information Protection Law 2021(PIPL) art 38 (China).

⁵⁰⁹ Personal Information Protection Law 2021(PIPL) art 39 (China).

⁵¹⁰ Personal Information Protection Law 2021(PIPL) art 40 (China)

transfers are only permitted after a security assessment by the State Cyberspace Administration.

4. Article 41⁵¹¹ stipulates that personal information stored in China may only be shared with other countries upon approval by Chinese authorities, ensuring compliance with domestic law and international agreements.

5. Article 42⁵¹² authorizes the State Cyberspace Administration to restrict cross-border data transfer for national security and public interest.

While the Personal Information Protection Law regulates private and corporate data use, it is explicitly silent on surveillance conducted by the state. Article 13 allows processing without consent for contract, legal duties, public health, emergency response, public interest, national security or handling publicly disclosed data. For Algorithmic Transparency and Automated Decision-Making, PIPL introduces notable provisions on automated decision-making in Articles 24 to 26. These articles mark China's first legislative attempts to regulate algorithmic governance. However, the law does not guarantee the right to human review, unlike GDPR. The enforcement of these provisions is also contingent on administrative priorities, limiting their practical empowerment.

1 Article 24⁵¹³ mandates that when a personal information processor uses automated decision-making, they must ensure transparency, fairness, and non-discrimination in outcomes. Individuals must be given non-personalized options or the ability to opt out of targeted decisions. If significantly impacted, individuals may request an explanation and reject automated decisions.

2. Article 25⁵¹⁴ stipulates that personal information processors are prohibited from disclosing personal data unless they obtain the individual's explicit consent.

⁵¹¹ Personal Information Protection Law 2021(PIPL), art 41 (China).

⁵¹² Personal Information Protection Law 2021(PIPL), art 42 (China).

⁵¹³ Personal Information Protection Law 2021(PIPL), art 24 (China).

⁵¹⁴ Personal Information Protection Law 2021(PIPL), art 25 (China).

3. Article 26⁵¹⁵ states that images and identification equipment in public places must serve public security needs, be clearly marked and cannot be used for other purposes without individual consent.

China views data as a national strategic resource, essential to AI leadership and digital trade independence. While PIPL facilitates regulated commercial use of personal data, it imposes strict compliance obligations on digital platforms. Under the PIPL, regulated yet commercially viable data flows are permitted, but only under a system of strict legal obligations imposed on data processors, especially major digital platforms. Key provisions of the PIPL are:

1. Article 6⁵¹⁶: Establishes the principle of data minimization, mandating that personal information must be processed lawfully, and to the minimum extent necessary for achieving the intended purpose.

2. Article 14⁵¹⁷: Requires that consent for data processing be informed, explicit, and freely given.

3. Article 58⁵¹⁸: It mandates heightened responsibilities for major internet platforms handling vast users' data and offering diverse services. Such entities must establish robust personal information protection compliance systems, including independent oversight bodies with external experts. It's required to create fair and transparent data governance rules, take corrective action against third-party service providers who violate privacy law, and issue regular social responsibility reports on data protection. These measures ensure stronger accountability and public trust in complex digital ecosystems.

The Personal Information Protection Law implicitly covers behavioural and emotional profiling through its regulations of *sensitive personal information* (Article 28), which includes sensitive personal information such as biometric details, religious beliefs, health records, financial accounts, and the location and identity of individuals

⁵¹⁵ Personal Information Protection Law 2021(PIPL), art 26 (China).

⁵¹⁶ Personal Information Protection Law 2021(PIPL), art 6 (China).

⁵¹⁷ Personal Information Protection Law 2021(PIPL), art 14 (China).

⁵¹⁸ Personal Information Protection Law 2021(PIPL), art 58 (China).

under 14 years. Processing such data is permitted only when clearly justified by a specific, necessary purpose and must be accompanied by enhanced protective measures to ensure its security and integrity. The recent Chinese regulation “*The Measures for the Security Management of the Application of Facial Recognition Technology*”⁵¹⁹ (2025) outlines strict obligations to safeguard algorithmic data. Article 5⁵²⁰ mandates that facial recognition must meet principles of legality, necessity, and minimal impact while performing facial data profiling. The regulation mandates that a prior personal impact assessment be required before processing facial data. The assessment must evaluate legality, risks, safeguards, and individual impact, and such should be retained for at least three years (Article 9⁵²¹). Furthermore, the regulation requires that the facial recognition system implement robust security measures, including encryption, access control and intrusion detection and comply with national cybersecurity obligations (Article 14⁵²²).

The obligations of a Data Fiduciary under the Personal Information Protection Law introduce accountability principles, resembling fiduciary duties, though it avoids normative terminology. Under PIPL :

1. Personal information must be processed lawfully, fairly, and only as necessary, without using deception, correction, or other improper methods (Article 5)⁵²³.
2. Personal information must be collected minimally and processed only for clear, reasonable purposes directly related to its use, ensuring the least possible impact on individual rights and interests (Article 6⁵²⁴).
3. Personal information must be processed transparently, with clear disclosure of processing rules, including its purpose, method, and scope (Article 7⁵²⁵).

⁵¹⁹ Measures for the Security Management of Facial Recognition Technology Applications, Cyberspace Administration of China, Ministry of Public Security of the People’s Republic of China, March 13, 2025, https://www.cac.gov.cn/2025-03/21/c_1744174262156096.htm (Last visited June 21, 2025).

⁵²⁰ Measures for the Security Management of Facial Recognition Technology Applications, (Cyberspace Administration of China, Ministry of Public Security), art 5 (2024).

⁵²¹ Supra note at 519, art 9.

⁵²² Supra note at 519, art 14.

⁵²³ Personal Information Protection Law 2021(PIPL), art 5 (China).

⁵²⁴ Personal Information Protection Law 2021(PIPL), art 6 (China).

⁵²⁵ Personal Information Protection Law 2021(PIPL), art 7 (China).

4. Personal information processors are accountable for their data handling and must implement necessary measures to ensure the security of the personal information.
5. No organization or individual may unlawfully collect, use, share or disclose others' personal information in ways that threaten national security.
6. Article 51 ensures lawful and secure processing, personal information processors must adopt comprehensive safeguards, including internal policies, data classification, technical measures like encryption, incident response plans, and legal compliance mechanisms. These obligations reflect an emerging data stewardship ethic, but the lack of individual enforcement weakens the fiduciary architecture.

The Personal Information Protection Law (PIPL) provides a foundational rights framework for data subjects, granting individuals the right to know, access, correct, and delete their personal information. PIPL grants several individuals rights under Articles 44 to 50, which are:

1. Right to be informed about and control the processing of their personal data, including the ability to limit or refuse its use, unless otherwise permitted by law.
2. Right to access, copy or request the transfer of their personal data.
3. Individuals may request correction or addition to their inaccurate or incomplete personal data, and processors are required to verify and update the information promptly.
4. The information processor must delete data when its processing purpose is fulfilled.

However, there is no express right to erasure for public interest data or any redressal mechanism independent of state agencies. Rights are legally recognized, but administratively controlled, reflecting the paradox of statutory empowerment within a non-liberal legal culture. China's regulatory approach to emerging technologies such as AI, IoT, and blockchain reflects a model of state-directed innovation, where technological advancement is encouraged within a tightly governed legal and ideological framework. The PIPL serve as the central legal foundation, applying to AI

systems that involve personal data by mandating a clear purpose limitation, individual consent and minimization. In parallel, the *Regulations on the Management of Algorithm Recommendations for Internet Information Services*⁵²⁶ (2022) focus on making algorithmic use fair, transparent, and accountable. Platforms must register recommendation algorithms, prevent discrimination, and avoid inducing addiction or harmful behaviour. Users should be able to opt out of personalized recommendations and access clear explanations of how algorithms work. This ensures that algorithmic technologies remain both socially accountable and politically aligned. The Blockchain Service Network (BSN), developed by China's National Information Centre and partners like China Mobile and UnionPay, offers a low-cost, accessible infrastructure for blockchain innovation. It helps organizations build and manage distributed applications efficiently and regulate blockchain development⁵²⁷. The BSN distributed cloud management platform helps governments, enterprises, and institutions run blockchain systems on their own cloud or local networks.

4.5 EMERGING CHALLENGES IN INTERNATIONAL DATA PROTECTION:

As nations strengthen their legislative frameworks on data protection and privacy, the global digital environment continues to evolve at an unprecedented pace. Technological advancements have introduced not only new opportunities for data-driven innovation but also complex regulatory dilemmas and ethical conundrums that transcend national borders. Existing laws, many of which were conceived in a pre-AI or pre-platform era, are now facing conceptual, operational, and jurisdictional strain. These developments call into question whether traditional privacy models grounded in consent, control, and fairness are adequate to address the structural shifts ushered in by automation and cyber-governance.

⁵²⁶ Regulations on the Management of Algorithm Recommendations for Internet Information Services, Ministry of Industry and Information Technology, dated 31st December 2021, https://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm (Last visited July 22, 2025).

⁵²⁷ Leader in distributed technology, builder of the Internet public layer, BNS, <https://www.bsnbase.com/> (Last visited June 21, 2025).

1. Artificial Intelligence and Automated Decision-Making

The rapid integration of Artificial Intelligence (AI) into decision-making processes, ranging from credit scoring to predictive policing and health diagnostics, has significantly disrupted traditional data protection paradigms. Automated decisions are often opaque and continuously challenge the very idea of data subjects exercising control over their personal data. Unlike a human actor, an algorithm does not provide reason in a conventional sense; its logic is embedded in code, optimization objectives, and training data that are often inaccessible to regulators and users alike.

2. Profiling, Surveillance and Emotional Data

The commodification of personal data has given rise to profiling technologies that sort individuals based on behavioural, emotional, or psychological attributes. These practices are prevalent in digital advertising, social media platforms, law enforcement, and even educational technology. Profiling, particularly when used for predictive analytics, raises profound concerns about discrimination, loss of autonomy, and manipulation. The challenge is not just legal epistemological how can law protect emotions, which are inferred and often invisible.

3. Global Cybersecurity Alliance and Privacy Dilution

In an era of escalating cyber threats, nation-states have increasingly aligned themselves in cybersecurity alliances and intelligence-sharing networks, such as the Five Eyes (US, UK, Canada, Australia, New Zealand)⁵²⁸, NATO Cyber Defence, or regional CERT collaboration in Asia. While such alliances are vital for coordinated threat response, they often operate with minimal transparency, oversight, or accountability regarding personal data shared across borders.

⁵²⁸ Five Country Ministerial, Public Safety Canada, <https://www.publicsafety.gc.ca/cnt/ntnl-scrf/fv-entry-mnstrl-en.aspx> (Last visited June 24, 2025).

4.6 CONCLUSION

The global legal architecture on data protection is a complex and evolving mosaic shaped by constitutional traditions and accelerating technological innovation. The international community is gradually coalescing around a shared recognition of informational privacy as a fundamental right, yet stark divergence remains in how states interpret, implement, and balance this right against competing interests such as national security, economic growth, and technological progress. The evolution of international norms in data protection from early OECD guidelines and soft law instruments to binding frameworks such as the EU GDPR and Convention 108+ reflects an increasing desire to establish global standards rooted in accountability, transparency, and user autonomy. Simultaneously, the rise of region-specific models, as seen in the GDPR, California's CPRA, South Korea's PIPA, South Africa's POPIA, China's PIPL and others, illustrates the necessity of context-sensitive adaptations. These regional laws differ not only in scope and enforcement but also in their philosophical underpinnings, ranging from right-based entitlement to consumer-centric frameworks, and in some cases, jurisdictions to state-managed informational sovereignty. The global rise of automated decision-making, surveillance technologies and cybersecurity alliances continues to strain the existing legal frameworks, calling into question the adequacy of traditional notions of consent and control mechanisms. In conclusion, the landscape of international data protection is at a pivotal crossroads. As data continues to influence economic power, political control, and individual autonomy, the task of regulation can no longer be viewed as a matter of statutory compliance alone; it must be approached as a constitutional and philosophical undertaking, one that demands coherence, imagination, and cross-border solidarity. The growing tension between privacy and national security often manifests in expansive surveillance power has underscored the urgent need for legal systems to reconceptualize privacy as a structural principle, not just an individual entitlement.

CHAPTER -5

CRITICAL APPRAISAL OF THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

5.1 INTRODUCTION

The *Digital Personal Data Protection Act 2023*⁵²⁹ (hereinafter referred to as DPDP Act) signifies a pivotal legislative intervention in India's journey towards constructing a coherent and contemporary data governance framework. Enacted in the wake of rising concerns about digital surveillance, data misuse, and technological opacity, the Act positions itself as the long-awaited statutory embodiment of the right to privacy recognized by the Supreme Court in *Justice K S Puttaswamy v Union of India*⁵³⁰ (2017). However, beneath its claims of protecting informational autonomy lies a complex and, at times, contradictory regulatory landscape. As the Indian state navigates between enabling economic growth through data flows and upholding individual freedoms in an increasingly digitalized public sphere, the DPDP Act 2023 emerges as both a milestone and a mirror; a milestone in legal codification and a mirror reflecting India's normative choices in the digital age. The chapter critically examines the Digital Personal Data Protection Act 2023 through a constitutional and rights-based lens. This chapter undertakes a comprehensive multilayered appraisal of the DPDP Act not merely as a statutory instrument but as a constitutional, ethical, and regulatory document that shapes the relationship between citizens, the state and the digital ecosystem. The objective is to evaluate whether the Act sufficiently safeguards the data rights of the individuals, aligns with the constitutional principles laid down by the Supreme Court and reflects the challenges posed by emerging technologies such as AI, IoT, blockchain and algorithmic governance.

⁵²⁹ The Digital Personal Data Protection Act 2023, (No 22), Act of Parliament, 2023 (India).

⁵³⁰ Justice K S Puttaswamy v Union of India (2017) 10 SCC 1, AIR 2017SC 4161.

The critical analysis of the chapter is anchored in three core dimensions that shape its evaluative framework. First, constitutional coherence of the Act, especially in light of the right to privacy, state accountability and informational self-determination. Second, it examines the institutional design and enforcement mechanisms, focusing on issues of independence, oversight, and procedural justice. Third, it explores the techno-legal and global regulatory dimensions, including cross-border data transfer regimes, digital trade norms and global comparative privacy frameworks. Structurally, the chapter is organized around ten key dimensions: (1) Constitutional recognition of the right to privacy (2) enforcement ecosystems, (3) Cross-border data transfer mechanisms, (4) surveillance, national security, and intelligence exceptions, (5) algorithmic transparency and automated decision-making, (6) intersection with digital trade and innovation ecosystems, (7) emotional and behavioural data exploitation, (8) obligations of data fiduciary (9) rights of the Data Principal and (10) regulation of emerging technologies including AI, IoT, and blockchain. These interwoven dimensions form the analytical foundation for evaluating the strengths, omissions and contradictions of the Digital Personal Data Protection Act 2023.

5.2 CONSTITUTIONAL RECOGNITION OF THE RIGHT TO PRIVACY

The legal philosophy underpinning data privacy in India finds its deepest roots in the Indian Constitution's guarantees of liberty, dignity, and equality. The constitutional embedding of the right to privacy as a fundamental right under Article 21, as affirmed by the Supreme Court in Justice K S Puttaswamy⁵³¹, has transformed the normative landscape of data governance in India. This jurisprudence sets a high constitutional bar for any law affecting data privacy. The Court articulated privacy as a composite right, encompassing bodily integrity, decisional autonomy, and informational control. Importantly, it established the triple test of ***legality, necessity, and proportionality*** for any infringement on this right, thereby creating a constitutional standard against which all data-related law must be evaluated.

⁵³¹ Justice K S Puttaswamy v Union of India (2017) 10 SCC 1, AIR 2017SC 4161.

5.3 GAPS IN LEGAL STRUCTURES AND SUBSTANTIVE PROVISIONS OF THE DPDP ACT 2023

While the Digital Personal Data Protection Act 2023 marks a legislative initiative in the domain of data governance in India, a closer scrutiny reveals serious limitations to the Act. The Act fails to deliver on this vision across several critical dimensions. First, it suffers from conceptual vagueness where key definitions are loosely defined; secondly, it neglects to adopt data classification tiers based on risk-based protection and third, the Act grants blanket exemptions to the State.

5.3.1 Vague and Underdefined Core Concepts:

A law that governs fundamental rights must be both clear and precise. This principle was affirmed by the Supreme Court in *Shreya Singhal v Union of India*⁵³²(2015), where section 66A of the IT Act was struck down on the grounds that vague terms violated Article 19(1)(a). The DPDP Act echoes similar conceptual vagueness in terms like “*lawful purpose*”, granting excessive discretion to enforcement authorities and data fiduciaries. Without elaboration, which can lead to varied interpretation across cases, making it difficult for individuals to know their rights have been violated or for regulators to enforce compliance consistency. The General Data Protection Regulation of the EU offers detailed technology-neutral definitions such as “*profiling*”, “*automated decision-making*”, and special categories of data. These ensure that the legal regime keeps pace with evolving digital risks. The Indian framework lacks this clarity, leading to a situation where individuals are subject to legal uncertainty, a direct violation of the constitutional requirement for clarity in laws that affect fundamental rights.

5.3.2 Absence of Data Classification Tiers

A structural flaw of the DPDP Act is its refusal to classify personal data into risk-based tiers, such as ‘*personal*’, ‘*sensitive*’, or ‘*critical data*’, and ‘*non-personal data*’. Different types of data attract different levels of protection based on the risk they pose.

⁵³² Shreya Singhal v Union of India- AIR 2015 SC 1523

This not only departs from international best practices but also ignores judicial expectations regarding proportionality in privacy regulation. The Act treats all data alike, whether it is a person's name or their genetic information. It renders the law ill-equipped to address domain-specific harm (e.g., in health, fintech or AI-based profiling). This creates a compliance vacuum and raises concerns about inadequate harm mitigation, especially in high-risk sectors. This one-size-fits-all model fails to recognize that certain kinds of data, if breached or misused, can lead to far more significant harm. Without tiered classification, the Act cannot implement proportionate safeguards, making it blind to the nuanced risk profiles of various sectors and technologies.

5.3.3 Unchecked State Power and Blanket Exemptions

Among the most troubling provisions of the DPDP Act is Section 17⁵³³, which empowers the Central Government to exempt any instrumentality of the State from the application of any or all provisions of the Act, on vaguely defined grounds such as national interest or sovereignty. These exemptions are not subject to judicial pre-clearance, legislative review, or time-bound oversight. Judicial guidance in *Menka Gandhi v Union of India*⁵³⁴ (1978), where the Supreme Court held that '*procedure established by law*' under Article 21 must be just, fair, and reasonable. These safeguards do not find blanket State exemptions under the DPDP Act. This creates an imbalance, allowing the very actor with the greatest surveillance capacity to operate outside the purview of privacy law.

⁵³³ The Digital Personal Data Protection Act 2023, (No 22), § 17 (2) The provisions of this Act shall not apply in respect of the processing of personal data (a) by such instrumentality of the State as the Central Government may notify, in the interest of sovereignty and integrity of India, security of the State, friendly relations with the foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these, and the processing by the Central Government of any personal data that such instrumentality may furnish to it;

⁵³⁴ *Menka Gandhi v Union of India*- 1978 SCR 621, AIR 1978 SC 597.

5.4 INSTITUTIONAL ECOSYSTEM AND ENFORCEMENT GAPS UNDER THE ACT

A rights-based data protection regime cannot function effectively without a robust, independent, and well-coordinated institutional framework. Laws alone do not secure rights, but institutions do. The DPDP Act introduces a new administrative body, the Data Protection Board of India (DPBI), which lacks the structural imagination and regulatory framework. This section critically examines four interrelated institutional lacunae that collectively weaken the Act's enforceability

5.4.1 Weak Institutional Design of the Data Protection Board

One of the most significant weaknesses of the DPDP Act lies in the design and mandate of the Data Protection Board of India. Under Section 18 of the Act, the Board is constituted by the Central Government, which also retains the power to determine its composition, functions, manner of selection, and even procedures, effectively making it an executive-controlled tribunal. This undermines the principles of institutional independence, separation of powers and regulatory autonomy. Yet the DPBI appears more as a bureaucratic entity than a quasi-judicial body. It lacks features typically associated with an independent data protection authority; no fixed qualification for its members, no transparent appointment process, no statutory guarantees of security of tenure, and no explicit requirement for technical or legal expertise in data governance⁵³⁵. Moreover, its powers are restricted to administrative inquiries, not comprehensive rule-making or advisory roles. In contrast, the EU Data Protection Board possess both enforcement and normative advisory functions.

5.4.2 Absence of Inter-Regulatory Coordination

Data protection in the 21st century is not a standalone regulatory function; it intersects with domains such as fintech, health tech, telecom and AI governance. In India, these

⁵³⁵ The Digital Personal Data Protection Act 2023, (No 22), §19 (3) The Chairperson and other Members shall be a person of ability, integrity and standing who possesses special knowledge or practical experience in the field of data governance, administration or implementation of laws related to social or consumer protection, dispute resolution, information and communication technology, digital economy, law, regulation or techno-regulation, or in any other field which in the opinion of the Central Government may be useful to the Board, and at least one among them shall be an expert in the field of law.

sectors are regulated by autonomous or semi-autonomous bodies like the Reserve Bank of India (RBI), Telecom Regulatory Authority of India (TRAI), and National Health Authority (NHA). However, the DPDP Act does not establish any formal mechanisms for inter-regulatory and coordinated decision-making.

5.4.3 *Inadequate Grievance Redressal Framework*

The DPDP Act prescribe that complaints first be submitted to data fiduciaries, and only thereafter, if unsatisfied, escalated to the Data Protection Board. Additionally, the Act does not establish a regional bench, ombuds mechanism, legal aid provisions or digital grievance portals in local languages, making it practically inaccessible for the rural and marginalized sections. It also lacks a clear appeal process to the judiciary for DPBI decisions.

5.5 CROSS-BORDER DATA TRANSFER MECHANISMS

The regulatory stance on cross-border data transfer, as articulated in the DPDP Act, reflects a notable departure from earlier data localization demands seen in the 2018 draft bill. Instead, the Act adopts a permissive but vague framework, wherein the Central Government will notify a list of countries or regions to which personal data can be freely transferred, without articulating any specific standards of “*adequacy*” or human rights protection. Most global data protection frameworks, such as the European Union’s GDPR Article 45⁵³⁶, permit cross-border data transfer is permitted only when the receiving country ensures an adequate level of data protection, assessed through a detailed legal and institutional analysis. This mechanism provides legal certainty for businesses and ensures that citizens’ rights are not diluted once their data crosses borders. The DPDP Act, however, omits any such structured adequacy criteria. There is also no mention of requiring reciprocal protections, judicial redress, or independent oversight mechanisms in the receiving country. This approach risks violating the principle of ‘privacy as a continuing right’ established in Justice K S Puttaswamy, which emphasized that privacy must be protected regardless of the

⁵³⁶ Supra note 386, art 45 transfers on the basis of an adequacy decision.

context or location of processing. Further, in the case of *Digital Rights Ireland Ltd v Minister for Communications*⁵³⁷ (CJEU 2014), the European Court of Justice invalidated the Data Retention Directives, holding that mass data transfer without adequate safeguards violates fundamental rights under the EU Charter. This sets a global precedent that legality and adequacy must guide cross-border transfer, an ethos absent in the Indian framework. The lack of clear data-sharing parameters, transition timelines, or adequacy benchmarks introduces legal and commercial risks under the DPDP Act 2023.

5.6 SURVEILLANCE, INTELLIGENCE AND STATE EXEMPTIONS

One of the most controversial and constitutionally sensitive features of the DPDP Act 2023 is its provisions for blanket state exemptions. The DPDP Act 2023 arrives at a moment when India's surveillance architecture remains largely governed by colonial-era law, such as the Indian Telegraph Act 1885⁵³⁸, and the Information Technology Act 2000⁵³⁹, both of which lack contemporary constitutional checks. The DPDP Act exempts the State from its key obligations, particularly in matters related to security, public order, and sovereignty. These exemptions are seeping, under-defined and devoid of procedural safeguards, raising serious concerns. Section 17 of the DPDP Act empowers the Central Government to exempt any state instrumentality, including intelligence, law enforcement or administrative bodies, from the application of any or all provisions of the Act. This includes exemptions from purpose limitations, consent obligations, notice requirements, storage limitations and access or correction rights for individuals. The justification supported for such exemptions revolves around sovereignty and integrity of India, security of the state and public order. However, these grounds are neither narrowly tailored nor procedurally bounded. Section 17 of the DPDP Act 2023 fails on multiple fronts:

- It delegates unchecked power to the executive without establishing a formal procedure.

⁵³⁷ *Digital Right Ireland Ltd v Minister for Communications* – C 293/12 and C-594-12 (2014).

⁵³⁸ Indian Telegraph Act 1885, (No. 13), Act of Parliament, 1885, (India).

⁵³⁹ Information Technology Act 2000, ((No. 21), Act of Parliament, 2000, (India).

- It lacks necessity or proportionality assessments.
- Data subjects are left with no rights or remedies against surveillance-driven violations.

5.7 ALGORITHMIC GOVERNANCE AND AUTOMATED DECISION-MAKING:

The DPDP Act was expected to address the growing influence of automated systems in personal data processing. However, the Act remains conspicuously silent on key challenges posed by AI-driven decision-making. It fails to define or regulate profiling, does not recognize any digital rights in the context of algorithmic harms, omits protections against emotional and behavioural data exploitations, and provides no risk-based regulatory framework for automated systems. This section evaluates these lacunae, focusing on four dimensions these are:

5.7.1 Lack of Legal Safeguards for AI Profiling

Profiling involves the use of personal data to evaluate aspects of an individual's life, such as preferences, behavioural, mental health, reliability, or economic status, often through automated or semi-automated systems. Despite the critical role profiling plays in automated governance, the DPDP Act fails to define, prohibit or regulate it. In contrast, the EU DGPR under Article 22 provides individuals with the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects. The GDPR also mandates transparency, impact assessments, and justification mechanisms for such decisions. In India, profiling has already emerged in several domains. The NITI Aayog's National AI Strategy promotes AI for governance⁵⁴⁰, while public schemes like Aadhaar-enabled Direct Benefit Transfer (DBT) and facial recognition in policing are increasingly driven by automated categorization. However, this concern has not been translated into statutory protection.

⁵⁴⁰ The NITI Aayog's National Strategy for Artificial Intelligence, AI for all, June 2018, <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf>.

5.7.2 Unrecognized Digital Rights in Automated Decision-Making Context

While the DPDP Act recognizes a basic set of rights, such as the right to access and correct personal data, but it fails to include rights specific to automated decision-making (ADM). There is no mention of the right to explanation, right to object, right to meaningful human intervention, or right to contest algorithmic decisions, all of which are increasingly accepted as essential digital rights in global jurisprudence.

5.7.3 Emotional and Behavioural Data Exploitation

The DPDP Act has no special protection for this category of data, despite its heightened sensitivity. Emotional data reflects internal states often unconsciously expressed, and its collection without consent or context can result in deep psychological intrusion.

5.7.4 No Risk-Based Regulatory Framework for Algorithms

The DPDP Act 2023, while a step forward in recognizing the importance of data privacy, fails to meaningfully address the realities of algorithmic governance and automated decision-making. In global AI regulation discourse, risk-tiered approaches are fast becoming the norm. The EU Artificial Intelligence Act 2024⁵⁴¹ classifies AI systems into ‘*unacceptable*’, ‘*high-risk*’ and ‘*limited-risk*’ categories, prescribing escalating obligations accordingly. Such frameworks help regulators prioritize resources and ensure proportionality in enforcement. However, India’s DPDP Act does not refer to algorithmic risk. Whether an AI system is used for public facial recognition or private advertising, it is treated identically under the law if addressed at all. Furthermore, there are no institutional roadmaps for sectoral co-regulation. The DPDP Act offers no guidance on coordination between data protection authorities and other relevant authorities in the context where AI is deployed, leaving India’s algorithmic governance ecosystem fragmented and reactionary.

⁵⁴¹ The EU Artificial Intelligence Act 2024, Regulation (EU) 2024/1689 of the European Parliament and of the Council, Notification dated 13th June 2024.

5.8 DATA FIDUCIARY DUTIES AND ACCOUNTABILITY MECHANISMS UNDER THE ACT

At the heart of any credible data protection regime lies a well-defined framework of duties for data fiduciaries, those entities that collect, process, and monetize personal data. These fiduciaries, both public and private, act as the primary custodians of data subjects' rights. The DPDP Act introduces the category of 'data fiduciary', conceptually inspired by the idea that those handling personal data owe a duty of care to data principals. The Act also grants the State excessive latitude in classifying '*Significant Data Fiduciaries*'⁵⁴² without normative criteria, raising concerns about unequal applications of obligations across sectors and actors. This section evaluates four interlinked issues:

5.8.1 *Limited Scope of Data Fiduciary Obligations-* Although the DPDP Act refers to the concept of a '*data fiduciary*', the obligations imposed under Sections 7⁵⁴³ and 8⁵⁴⁴ are procedural in form and minimal in substance. Fiduciaries are required to obtain consent, implement security safeguards and report breaches. However, the Act stops short of articulating ethical or trust-based responsibilities, which are the hallmarks of fiduciary doctrine. Unlike the EU GDPR, which introduces principles of data minimization, purpose limitation, fairness and accountability, the DPDP Act 2023 offers no guiding principles. It treats fiduciaries as technical actors rather than moral agents entrusted with autonomy-altering decisions.

5.8.2 *Lack of Procedural Fairness in Data Processing-* Any legal process, especially those affecting fundamental rights, must uphold the principles of natural justice and procedural fairness. This includes the right to notice, hearing, access to information, and opportunity to contest. However, the DPDP Act does not mandate fiduciaries to inform individuals how their data will be processed, which algorithms are involved, or what outcomes may result, thus violating the *audi alteram partem* principle.

⁵⁴² The Digital Personal Data Protection Act 2023, (No 22), § 10(2) India.

⁵⁴³ The Digital Personal Data Protection Act 2023, (No 22), § 7, India.

⁵⁴⁴ The Digital Personal Data Protection Act 2023, (No 22), § 8, India.

5.8.3 No Sector-Specific Accountability Provisions- Data is not uniform in character; different data differ in risk and sensitivity. Similarly, different categories of data require data handling practices that raise different concerns compared to law enforcement systems. However, the DPDP Act impose a uniform set of fiduciary duties, without acknowledging the risk diversity across sectors. Furthermore, the Act does not compel inter-agency collaboration between the Data Protection Board and regulators like the RBI, SEBI, NHA or TRAI, leading to fragmented oversight. The DPDP Act misses this harmonization opportunity, resulting in compliance confusion, regulatory gaps and a lack of coordinated redress mechanisms.

5.9 RIGHTS OF THE DATA PRINCIPAL

The DPDP Act introduces a basic rights framework for data principles, but this section examines three key lacunae in the empowerment framework under the Act:

5.9.1 Incomplete Recognition of Individual Rights

The DPDP Act grants data principals a set of five core rights (i) the right to access personal data, (ii) the right to correct or erase inaccurate data, (iii) the right to nominate, (iv) the right to grievance redressal and (v) the right to withdraw consent. while these are necessary, they are necessary, they are insufficient in both scope and enforceability. In contrast, the EU GDPR guarantees a broader set of rights, including the right to data portability, the right to object to processing, the right to restriction and rights against automated decision-making.

5.9.2 Right to Data Portability and Right to Objection

The most glaring omission in the DPDP Act is the right to data portability and the right to object to processing. Data Portability enables individuals to transfer their personal data from one platform or service provider to another, empowering user choice. The Right to object, on the other hand, allows users to challenge data processing that they believe is intrusive, unfair or excessive. These rights are essential to mitigate algorithmic profiling, targeted advertising, and automated decision-making.

5.9.3 *Lack of Collective and Community Data Rights*

The DPDP Act is the complete absence of collective and community data rights. In India is not just about the individuals; it often emerges from collective social experience, such as indigenous knowledge systems. Yet the DPDP Act does not create any space for tribal councils, community-based organisation to claim their collective informational resources.

5.10 REGULATING EMERGING TECHNOLOGIES: AI, IoT, BLOCKCHAIN:

The future of digital society is inseparably tied to emerging technologies from artificial intelligence (AI), and the Internet of Things (IoT), to distributed ledger systems like blockchain. These technologies are not merely tools; they redefine how data is generated, processed, circulated and acted upon. They also blur traditional legal distinctions between controller and processor, subject and object, and even consent and interference. A modern data protection law must therefore anticipate and adapt to technological evolution.

5.10.1 *Regulatory Silence for IoT and Device-Generated Data-* IoT (Internet of Things) systems generate data not through direct user input interaction, but through passive sensors, wearable devices, home automation, vehicle telemetry, and industrial monitoring. This data is often ambient, continuous, and non-consensual in nature, raising profound concerns about opacity, control and privacy intrusion. However, the DPDP Act does not address device-generated data as a separate category. It does not extend to inferred or predictive data that IoT systems generally generate.

5.10.2 *Incompatibility with Blockchain Technology-* Blockchain and distributed ledger technologies are based on principles that challenge many foundational ideas of conventional data protection law. These systems deliberately make data non-erasable and non-editable to create tamper-proof records. The Act does not offer any guidance for how such rights could be exercised in a blockchain-based environment, raising serious concerns for data subjects whose personal data may be recorded on the chain.

5.10.3 No Regulation for High-Risk AI Systems- Globally, jurisdictions are converging on the need to identify and regulate high-risk AI applications. The EU's AI Act, for instance, mandates risk-tiered obligations, algorithmic impact assessments, human oversight, and strict rules for prohibited uses, such as social scoring. The DPDP Act, in contrast, does not even mention AI, machine learning, or algorithmic systems. There are no provisions for assessing risk or conducting audits. The absence of AI-specific safeguards, especially for high-risk deployments, means the DPDP Act fails to recognize the unique harm potential of these systems.

5.11 DATA LOCALIZATION AND DATA BREACH NOTIFICATION

One of the most debated features of earlier drafts of India's data protection framework was the proposed data localization mandates, which require the storage of personal data within the territory of India. Justice B N Krishna Committee Report (2018) had recommended a local copy mandate for all personal data and strict localization for critical personal data, emphasizing data sovereignty, national security and law enforcement access. However, the DPDP Act 2023 abandoned this rigid localization approach and instead adopted a transfer approval model. There is no general obligation under the Act to store or process data exclusively in India. The Act permits cross-border transfer by default, unless the receiving jurisdiction is not on the approval list. Regarding data breach notification, a fundamental feature of modern data protection law is the requirement to notify data breaches in a timely and transparent manner, ensuring that individuals can take precautionary steps to protect themselves from harm. The obligation to notify both the Data Protection Board and affected data principals is a positive obligation. However, the timeline, form and threshold of harm that trigger notification are not specified in the Act itself and are left to future rules prescribed by the Executive. The Act does not obligate fiduciaries to assist affected users, nor does it offer a clear redress mechanism to challenge underreporting or delay. The breach notification mechanisms are not linked to the right to access, correction or erasure. Thus, even if a breach occurs, data principals may not receive adequate context to assert or enforce their rights.

5.12 COMPARATIVE STUDY OF THE DIGITAL PERSONAL DATA PROTECTION ACT 2023 WITH GLOBAL LEGISLATION

In an era where data flows transcend national borders, the effectiveness and legitimacy of domestic data protection are measured not in isolation but in comparison with global norms and standards. Every country's data protection framework is shaped by transitional norms, trade agreements and the global flow of data and influences. This section explores a structured comparative analysis of the DPDP Act alongside leading global frameworks. It seeks to benchmark India's law against these instruments, not merely to identify gaps, but to explore the areas that were missed in institutional design and regulatory divergence.

1. The EU General Data Protection Regulation and the DPDP Act 2023

The General Data Protection Regulation⁵⁴⁵ of the EU continues to set the global benchmark for comprehensive and rights-centric data protection. Anchored in principles such as lawfulness, fairness, transparency, purpose limitations, and data minimization. It offers a sophisticated and enforceable framework for both individuals and regulators. Notable features of GDPR are the right to explanation and objection to automated decision-making (Article 22), data portability (Article 20), and mandatory impact assessments for high-risk processing activities (Article 35), which reflect the GDPR's commitment to balancing technological innovation with individuals' autonomy. The independence of Data Protection Authorities (DPAs) and implementation of the 'One-Stop Shop' mechanism for cross-border grievances underscore their institutional robustness and user accessibility. In contrast, India's Digital Personal Data Protection Act 2023 adopts a significantly diluted approach. It lacks the right to data portability, provides no statutory guarantee of algorithmic accountability, and omits any requirement of Data Protection Impact Assessment, even in the context involving high-risk or sensitive data processing. Furthermore, the establishment of a government-controlled Data Protection Board undermines the principle of institutional independence.

⁵⁴⁵ Supra note 386

2. *California Privacy Rights Act and the DPDP Act 2023*

California's Consumer Privacy Act⁵⁴⁶ (CCPA), significantly strengthened by the California Privacy Rights Act⁵⁴⁷ (CPRA), represents a progressive, consumer-first model of data protection within the United States. It empowers individuals with rights such as the right to opt out of the sale of personal data, the right to know what data is collected and for what purposes, and the right to request deletion. One of its most significant advances is the recognition and special treatment of '*sensitive personal information*', including race, precise geolocation, health data and biometrics, making higher levels of disclosure and control. Enforcement of these rights is entrusted to a purpose-built, independent regulator, ensuring that rights are not merely theoretical but actively enforced. In contrast, India's DPDP Act 2023 takes a more limited and compliance-heavy approach. It does not offer individuals the ability to opt out of profiling, targeted advertising, or data monetization practices. Moreover, the Act does not explicitly distinguish between general personal data and sensitive personal data, thereby missing an opportunity to impose enhanced safeguards for high-risk information. This lack of granularity limits both the protective scope of the law and its alignment with international standards. Additionally, the absence of a sector-neutral, independently empowered enforcement body further weakens the rights-enforcement ecosystem under the DPDP Act.

3. *Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) 2000 and the DPDP Act 2023*

Canada's Personal Information Protection and Electronic Documents Act 2000⁵⁴⁸ represents an early and internationally respected effort to regulate the collection, use and disclosure of personal data in the context of commercial activities. Grounded in ten fair information principles, PIPEDA emphasizes a risk-based, accountability-centric model that requires organizations to obtain consent, ensure transparency and

⁵⁴⁶ California Consumer Privacy Act 2018, California Civil Code [1798.100- 1798.199.100].

⁵⁴⁷ The California Privacy Right Act 2020 came into effect from 1st January 2023.

⁵⁴⁸ Personal Information Protection and Electronic Documents Act 2000, (SC 2000, c.5) April 13th, 2000, <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/>, (Last visited July 26, 2025).

implement safeguards proportionate to the sensitivity of the data involved. Enforcement is entrusted to the Office of the Privacy Commissioner (OPC), an independent body with investigatory and advisory powers. The recent proposal of Bill C-27⁵⁴⁹ (CPPA) seeks to modernize the regime by introducing stronger oversight, provisions for algorithmic transparency, and clear standards for data de-identification. PIPEDA applies primarily to the private sector, while the public sector is governed under separate legislation. By contrast, India's DPDP Act 2023 establishes a more centralized compliance-oriented framework that applies to both private and public sector entities, including government departments and law enforcement agencies. While the PIPEDA reflects an evolving commitment to individual rights and independent oversight, the DPDP Act adopts a state-centric model that prioritizes administrative control over substantive privacy protections.

4. South Korea's Personal Information Protection Act and the DPDP Act

South Korea's Personal Information Protection Act 2011⁵⁵⁰ is widely acknowledged as one of the most robust data protection regimes in Asia, often praised for its closer alignment with the EU GDPR. PIPA is built on a foundation of strong consent requirements, imposes strict conditions on cross-border data transfer, and requires explicit consent and evidence of adequate protection in the recipient country. At the institutional level, the independent Personal Information Protection Commission has the authority to investigate breaches, enforce compliance, and issue sanctions. In stark contrast, India's DPDP Act 2023 delegates the critical responsibilities of cross-border data transfer governance entirely to the executive, without laying down clear statutory criteria or procedural safeguards. This opaque notification-based model raises concerns about the arbitrariness and regulatory uncertainty, particularly for businesses and citizens relying on international data flows.

⁵⁴⁹ Bill C 27- An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, Current Status is at consideration in Committee in the House of Commons, available at: <https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading> (Last visited July 26, 2025).

⁵⁵⁰ Personal Information Protection Act 2011, (No 10465) dated 29th March 2011, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG, last amended by Act no. 19234 on 14th March 2023, https://elaw.klri.re.kr/eng_service/lawView.do?lang=ENG&hseq=62389.

5. *China's Personal Information Protection Law (PIPL) and the DPPD Act*

China's Personal Information Protection Law 2021⁵⁵¹ (PIPL) represents one of the most comprehensive data protection frameworks in the Global South, combining strict compliance obligations with strong state oversight. Despite being rooted in a model of centralized governance, the PIPL offers a detailed and structured approach to regulating personal data. It mandates categorization of sensitive personal data, requires companies to appoint Data Protection Officers, and imposes explicit consent requirements and risk assessments for high-risk practices such as automated profiling. Moreover, its localization rules for Critical Information Infrastructure ensure that strategically sensitive data is stored and processed within national borders, reflecting a policy of digital sovereignty with legal accountability. These provisions demonstrate China's attempt to assert regulatory control while also demanding a high degree of corporate compliance through obligations and robust enforcement. The DPDP Act 2023, by contrast, avoids stringent data localization mandates. The DPDP Act lacks penalty gradation based on the severity of violations and does not impose mandatory data protection officers or risk-based audits for high-risk data processing. There are no legal requirements for companies to conduct algorithmic risk assessments, even when engaging in profiling, targeted advertising, or automated decision-making.

⁵⁵¹ Personal Information Protection Law 2021(PIPL) People's Republic of China (NPC) dated 20th August 2021, <https://personalinformationprotectionlaw.com/>.

Table 5.1: Comparative Analysis of DPDPA Act with Global Data Protection Laws

Aspects	EU GDPR	California (CCPA/CPRA)	Canada (PIPEDA / CPPA draft)	South Africa (POPIA)	South Korea (PIPA)	China (PIPL, DSL, CSL)	India (DPDP Act 2023)
1. Right to privacy	EU Charter of Fundamental Rights	No constitutional right	Charter rights (privacy) evolving in the CPPA draft	Constitutionally aligned	Rooted in constitutional privacy protections	Collectivist & state-security-driven	No explicit constitutional privacy right, but the SC recognized
2. Enforcement Ecosystems	Independent DPAs + EDPB	California Privacy Protection Agency (CPPA)	Office of Privacy Commissioner (OPC)	Information Regulator	Personal Information Protection Commission (PIPC)	CAC and multiple sectoral regulators	Data Protection Board of India (DPBI)
3. Cross-Border Data Transfer	Adequacy, SCCs, BCRs	No adequate contractual business safeguards	Adequacy & contractual clauses (draft CPPA)	Restrictions & contractual clauses	Adequacy-based & contractual safeguards	Strict localization & security review (PIPL, DSL)	allowed with govt. notification & possible restriction
4. Surveillance & Exceptions	Limited but proportionality principle	Broad exemptions for law enforcement	National security carve-outs	State security exception	Exceptions for public safety/national security	Expansive state security overrides individual rights	Broad exemptions for sovereignty, security, and public order
5. Algorithmic & Automated Decision-Making	Right not to be subject to solely automated decisions	Limited transparency obligations	Weak in PIPEDA, stronger in CPPA draft	Limited, weak explicit rights	Specific rights against automated processing	Obligations on transparency + security, limited individual challenge rights	not explicitly integrated
6. Intersection with Digital Trade & Innovation Ecosystems	Integrated with the EU digital single market, AI Act, DSA	Balances consumer rights and business innovation	Strong digital economy focus (esp. CPPA draft)	not explicitly integrated	Integrated with a strong ICT sector	Strong linkage with AI, data localization, and trade rules	Interoperability is not explicitly integrated
7. Algorithmic Governance	Explicitly protects special categories	Covers sensitive personal data but is limited	Not deeply covered; biometric data partially	Sensitive data categories covered	Covers sensitive & biometric data	Explicit rules for sensitive, incl. biometric & health	Not covered
8. Obligations of Data Fiduciary	Strong obligations (lawful basis, accountability, DPIAs)	Businesses = covered entities with consumer duties	Accountability principle; draft CPPA strengthens fiduciary duties	Responsible party duties	Strong fiduciary/accountability framework	Data handlers = strict duties with state oversight	Significant data fiduciaries face higher obligations
9. Rights of Data Principals	access, rectification, erasure, portability, objection	Access, deletion, opt-out, correction (CPRA expands)	Access, correction, portability (weaker than GDPR)	Access, correction, and deletion rights	Broad rights, close to GDPR	Rights exist but are limited against state power	consent, erasure, correction grievance redress, nomination
10. Emerging Technologies	Linked with AI Act, ePrivacy, DSA	No AI-specific law, but CPRA addresses profiling	CPPA draft expands to AI/automated decision-making	Not explicitly covered	Active regulation in AI/ICT	Strong AI, algorithm, and blockchain oversight	Not explicitly covered

5.13 LIMITATIONS OF DIGITAL PERSONAL DATA PROTECTION RULE 2025

The Digital Personal Data Protection Rule 2025⁵⁵² was notified under the enabling provisions of Section 40 of the Digital Personal Data Protection Act 2023, providing the operational framework for India's data protection regime. These Rules hold immense interpretative significance. They give shape to broad statutory provisions and form the backbone of compliance, enforcement and rights assertions under the Act. However, the Digital Personal Data Protection Rule 2025⁵⁵³ also contains certain limitations, such as:

1. Excessive Government discretion (Rules 15 & 23)

One of the weaknesses of the Digital Personal Data Protection Rules 2025 is the wide discretionary power of the Central Government in the provisions of Rules 15 and 23. Rule 15 permits cross-border data transfers with conditions as may be specified, not converting to express standards, thus breeding uncertainty and executive hubris. Which is associated with Rule 23, but allows the broad-handed requirement of information, is a rule of the Seventh Schedule. Sub-rule (2) allows non-disclosure of such requests on the grounds of sovereignty or security, making it less transparent. Due to the absence of procedural safeguards or independent oversight, arbitrariness risks increase, affecting accountability and confidence in the regulatory structure.

2. Absence of Clear Standard (Rules 15 & 13)

Data Protection Rules, 2025, exude a clear absence of a precisely defined standard, as it is based on executive specification. Even though Rule 13 provides outlined requirements like annual Data Protection Impact Assessment and audit and

⁵⁵² The Draft of rules proposed to be made by the Central Government in exercise of the powers conferred by subsection (1) and (2) of section of the Digital Personal Data Protection Act 2023 (Act no 22 of 2023), on or after the date of coming into force of the Act, are published by the Ministry of Electronics and Information Technology published for the information of all persons likely to be affected thereby; Notification dated 3rd January 2025, <https://cdn.digitalindiaincorporation.in/wp-content/uploads/2025/01/Draft-Digital-Personal-Data-Protection-Rules2025.pdf>

⁵⁵³ DIGITAL PERSONAL DATA PROTECTION RULES 2025, GSR 846 (E.), (India) Nov. 13, 2025, <https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf>.

algorithmic due diligence, sub-rule (4) leaves the Central Government with the discretion of determining groups of personal data that bring about localization. This introduces uncertainty about the scope of compliance. This worry is heightened in Rule 15, which puts the cross-border data transfers subject to conditions that may be stipulated by the government. This lack of objective criteria creates ambiguity, executive discretion, and inconsistency in its implementation, and complicates the development of predictable and sustainable compliance strategies by data fiduciaries.

3. Weak Enforcement of the Data Principals of Rights (Rule 14)

Data Principal rights are exercised via Rule 14 of Data Protection Rules 2025, which mainly depends on Data Fiduciaries through the mechanisms provided, hence largely relying on the internal systems. Although the rule obliges to publish access procedures and offers a redressal grievance framework, it grants an opportunity of up to ninety days to resolve them, which might be unreasonable in instances where privacy is an urgent matter. In addition, the rule lacks the element of independent oversight in its structure, which may hamper the sense of accountability. Consequently, despite being formally acknowledged and operationalized by Rule 14, Data Principal rights may be impacted in terms of their importance, objectivity, and expediency in their enforcement in practice, owing to the inclusion of fiduciary-controlled processes.

4. Wide Exemptions and their impact on Privacy Protections (Rules 5, 12 and 16)

Various conditional exemptions are included in the Data Protection Rules, 2025, in the Form of Rules 5, 12, and 16, which can potentially compromise the strength of privacy protection. Rule 5 allows processing by the State to deliver subsidies and services based on such standards as specified in the Second Schedule, and Rule 12 exempts data processing related to children under certain specified conditions. Likewise, Rule 16 does not apply the Act to research and statistical processing in situations where standards prescribed are observed. Despite the valid purposes of these provisions, the use of broadly-worded schedules and the conditional safeguards can lead to interpretation flexibility and undermine fundamental principles, including data minimisation and purpose limitation and blur the overall protective process.

5. Insufficient Autonomy of Data Protection Board (Rules 17 & 18)

The Data Protection Board structure, in which the institutional framework applies especially in Rules 17 and 18, demonstrates a large extent of control by the executive in terms of appointments and terms of service. The Central Government is dominant in forming the Board and stipulating the terms of the members. The lack of an independent or judicial appointment process creates issues of independence and objectivity of the Board.

6. Small and Medium Data fiduciary challenges to compliance.

The mandatory requirements of Rules 6, 7 and 8 have standardized and technically challenging requirements on all Data Fiduciaries, potentially unduly burdening small and medium enterprises. In Rule 6, vast security protection is provided, such as encryption, access controls, and retention of logs, and in Rule 7, breaches must be promptly notified to both individuals affected and the Board. Rule 8 also dictates the deadline for erasing data and the obligatory maintenance of the logs. Even though these steps improve data protection, the lack of a proportionate or tiered compliance system does not consider the organizational capacity difference, which can be a huge imposition on small organizations and their involvement in the digital economy.

7. Algorithmic and AI Governance Regulatory gaps (Rule 13)

The Data Protection Rules, 2025, in rule 13 place some requirements on Significant Data Fiduciaries, such as performing Data Protection Impact Assessment and practising due diligence to ensure that the algorithmic systems do not have negative impacts on the rights of Data Principals. The rule, however, has a narrow and risk-oriented strategy, and it does not give the specific normative regulations of new technologies like artificial intelligence or automated decision-making. It does not specifically note important factors like transparency, explainability, or algorithmic accountability. Such a lack of detailed guidance can potentially permit opaque decision-making procedures to continue, emphasizing the importance of a more detailed and future-oriented regulatory framework.

8. Data Retention and Erasure Policies (Rule 8) are ambiguous.

The Data Protection Rules 2025, Rule 8 provides a systematic data retention and data erasure framework that stipulates that personal data has to be deleted within a certain time frame, but data on logs must be kept for a minimum of one year. The combination of an obligation of erasure, an obligation of advance notice and an exception that it satisfies other laws or government notifications, this leads to operational complexities. Data Fiduciaries might not even know when the right time to dispose of data should be, especially in cases where there is overlapping legal coverage. This stratified strategy can lead to inconsistencies in its practice and provoke questions about compliance with such principles as data minimisation, which means that better and more coordinated retention policies should be made.

5.14 BRIDGING THE GAPS: PATHWAYS FOR POLICY REFORM

The enactment of the Digital Personal Data Protection Act 2023 and the DPDP Rule 2025 show India's formal entry into the age of data governance. However, as this chapter has demonstrated, the current regime is shaped by limited rights articulation, executive-dominated institutions and a compliance-oriented philosophy that prioritizes procedural form over normative substance. The following approaches can be adopted to bridge the gaps

5.14.1 Institutional Innovation and Structural Reforms: The effectiveness of any data protection regime rests not just in rights or rules, but in the institutions that interpret, enforce and embody them. The current Data Protection Board lacks the independence, transparency, and diversity necessary to act as a counterbalance to both state and corporate power. **Creation of a multi-tiered grievance redressal structure, including**

- i. Regional breaches for linguistic and digital accessibility
- ii. Ombudsperson model with the power to issue binding orders
- iii. Mandated coordination with sectoral regulators (RBI, TRAI, NHA, etc.) through Joint Regulatory Committees.

5.14.2 Risk-Based and Rights-Based Processing System: Current data processing cannot be governed by static or uniform rules. Instead, it requires a risk-based, context-sensitive system that aligns compliance obligations with the sensitivity of data, the scale of impact and vulnerability of the data subjects:

i. Classification of data based on Risk

- Tier I: Basic identifies (e.g., name, contact)
- Tier II: Sensitive Personal Data (eg, health, financial, religion, etc.)
- Tier III: High-risk data (e.g. biometric, emotional behavioural)

ii. Algorithmic Risk Assessments:

- Mandate AI Impact Assessments
- Right to Opt-out Profiling

5.14.3 Enforcement Ecosystems: The Data Protection Board of India is a quasi-independent authority to adjudicate data breaches and impose penalties. This model undermines institutional autonomy. Comparative models like the EU Data Protection Board and the UK Information Commissioner's Office function with greater independence. Further, this can be improved by:

- Statutory independence of the DPBI.
- Empower the Board to issue binding codes of practice and establish frameworks for emerging technologies.

5.14.4 Cross-Border data transfer: The Act adopts a government-notified whitelist approach, allowing personal data transfer only to countries approved by the Central Government. Existing cross-border data transfer frameworks required:

- Replacing the whitelist model with a risk-based adequacy framework.
- Introducing Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs) to ensure interoperability with the global data ecosystem.
- Digital Trade Facilitation Agreements to prevent data localization barriers while ensuring privacy protection.

5.14.5 Algorithmic Transparency and Automated Decision-Making: The DPDP Act is currently silent on automated decision-making (ADM) and profiling and algorithmic bias. Without provisions for algorithmic transparency, individuals have no right to explanation or contestation against AI-driven profiling. So, there is an urgent need to

- Introduce a “*right to explanation*” for decisions made based on AI-driven.
- Mandate algorithmic impact assessment (AIA) and human oversight in the decision-making process.
- Require disclosure of data training sources.

5.15 CONCLUSION

The Digital Personal Data Protection Act 2023 represents an important step forward in India’s attempt to regulate the fast-evolving terrain of digital life. It introduces a long-awaited legal framework for personal data, consent mechanism, notice, fiduciary responsibility and procedural safeguards. Yet, as this chapter has critically revealed, the DPDP Act falls short in certain aspects. The analysis has identified multiple structural limitations, ranging from vague definitional frameworks, executive-controlled exemptions, minimal procedural safeguards, absence of algorithmic rights, institutional independence and sectoral regulations. After comparing the DPDP Act with the global laws on data protection, it shows how other jurisdictions have embedded data dignity and algorithmic transparency more efficiently. As emerging technologies like AI, IoT and blockchain reshape the terrain of data flows and control, the need for a second-generation data protection framework becomes evident. In sum, the DPDP Act 2023 is a beginning but not yet a culmination. Its critical appraisal reveals both the promise and perils of India’s digital data governance framework.

CHAPTER -6

ASSESSING THE APPLICABILITY OF DATA PROTECTION LAWS IN THE STATE OF NAGALAND: AN ANALYSIS

6.1 INTRODUCTION

In the era of digital transformation, personal data has emerged as one of the most valuable resources, shaping governance, commerce, and individual interactions. India's rapid shift towards a digital economy has redefined how personal data is collected, stored, processed and shared, leading to both opportunities and challenges. As data becomes central to decision-making processes in both public and private sectors, questions concerning the protection of individual privacy, the ethical use of data and the accountability of data handlers have gained unprecedented prominence. In response to this, the enactment of the Digital Personal Data Protection Act 2023 marked a significant legislative step in India's evolving data governance regime, aiming to regulate the processing of personal data and uphold the principles of transparency, consent, and protection. The chapter seeks to assess the applicability of India's data protection laws in Nagaland through an integrated doctrinal and empirical analysis. The doctrinal dimensions focused on examining the constitutional, legislative and judicial foundations that determine how central data protection laws operate within the State. The empirical dimension complements this by exploring the practical realities of data protection within the State, how institutions manage data, how compliance mechanisms operate, and how citizens perceive the value of privacy in their digital rights.

This chapter deals with the applicability of the Digital Personal Data Protection Act 2023 in the context of the State of Nagaland, guided by the research question and hypotheses of the study. It seeks to determine whether the national data protection framework, designed to safeguard personal data and privacy rights, can be effectively enforced in Nagaland. The chapter begins with a demographic overview of respondents, followed by hypothesis testing and answers to the research questions.

It further develops a contextual framework for assessing the Act’s applicability. The conclusion synthesizes these findings to determine whether the Digital Personal Data Protection Act 2023 can be effectively implemented in Nagaland or whether localized adaptations are necessary to align the law with the State’s unique socio-legal context.

6.2 DEMOGRAPHIC PROFILE OF THE RESPONDENTS

The demographic profile of the respondents includes age groups, gender, educational qualification and occupation of 400 respondents. The diversity in age, education, and occupation helps in understanding variation in digital literacy and privacy awareness across social groups.

i. Age Distribution: The age profile of respondents reveals that a significant majority, 77.5% (n= 310), belongs to the 18- 25 years age group. This indicates that the larger representation is by the young individuals, most likely students and earlier-career professionals. The 26-35 years group is 14.8%, followed by the 36-45 years 6.8%, and only 1% falls in the 46-60 years bracket. Table 6.1 represents the age distribution of the respondents.

Table 6.1 Respondents age distribution

Age Group	Frequency	Percentage
18-25	310	77.5 %
26-35	59	14.8 %
36-45	27	6.8 %
46-60	4	1.0 %
Total	400	100 %

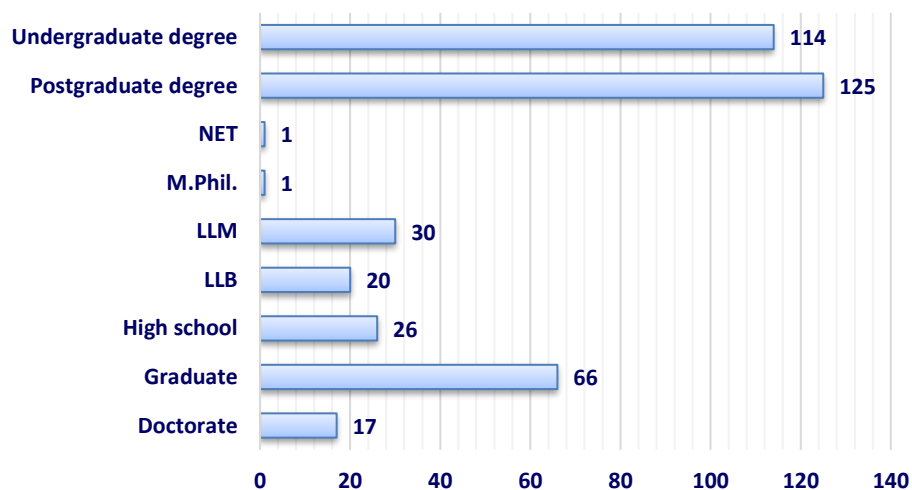
ii. Gender Distribution: In terms of gender, the sample is fairly balanced. Out of the total respondents, 51.8% (n=207) are females and 47.3% (n=189) are males, while 1% (n=4) preferred not to disclose their gender. Table 6.2 presents the gender distribution of the respondents.

Table 6.2: Gender distribution of respondents

Gender	Frequency	Percent
Female	207	51.8 %
Male	189	47.3 %
Prefer not to say	4	1.0 %
Total	400	100 %

iii. Educational Qualification: The educational background of respondents demonstrates a well-educated sample group. A considerable proportion, 31.3% (n=125), hold a postgraduate degree, followed closely by 28.5% (n=114) with an undergraduate degree, 16.5% (n=66) are graduates, while 6.5% (n=26) have completed high school. A smaller fraction holds professional or advanced qualifications such as LLB (5 %), LLM (7.5%), Doctorate (4.3%), M.Phil. (0.3%) and NET (0.3%). The data highlights that most participants possess higher education. Figure 6.1 shows the educational qualifications of the respondents.

Figure 6.1 Educational Qualifications of the respondents



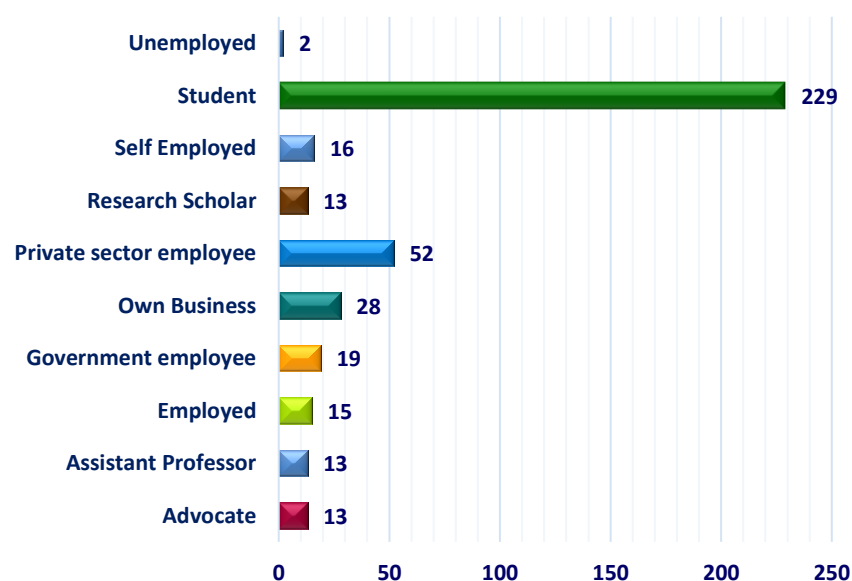
iv. Resident: The residential distribution indicates that a vast majority, 91% (n = 354), are residents of Nagaland, while only 9% (n = 36) are from other states.

Table 6.3 Residence of the respondents

Resident	Frequency	Percent
Nagaland	364	91 %
Other	36	9 %
Total	400	100 %

v. Occupational Status: The analysis of occupational status shows that the majority of respondents are students, comprising 57.3% (n=229) of the sample. Among the employed categories, private sector employees 13% (n=52), business owners (7%), government employees (4.8%), and self-employed individuals (4%). The smaller segment includes (3.3%), assistant professors (3.3%), research scholars (3.3%) and only 0.5% (n=2) reported being unemployed. Figure 6.2 represents the occupational status of the respondents.

Figure 6.2 Occupational Status of Respondents



6.3 PEOPLE'S UNDERSTANDING OF DATA PRIVACY AND RIGHTS:

The people's understanding of Data Privacy and Protection, which explores the level of awareness, perception, and attitude of citizens towards data privacy in Nagaland. This dimension recognizes that the effectiveness of any data protection regime, no matter how robust its legal framework, ultimately rests upon the informed participation of individuals whose data is being collected and processed. The DPDPA 2023 emphasizes the principles of informed consent and data subject empowerment; however, these principles can be meaningfully realized when citizens possess a clear understanding of their rights. The detailed analysis of people's perceptions and understandings of data privacy and rights is as follows:

1. *Familiarity with the term "Data Protection"*

The survey result reveals varying degrees of familiarity with the concept of data protection among the respondents. 15.8% (63) reported being "*not familiar*", 66% (264) indicated that they were "*somewhat familiar*", and 18.2% (73) stated that they were "*very familiar*". The level of familiarity with the term "*data protection*" serves as a starting point for understanding the broader spectrum of public awareness about privacy and rights. Figure 6.3 represents the familiarity with the term data protection, and Table 6.4 presents the familiarity across age groups.

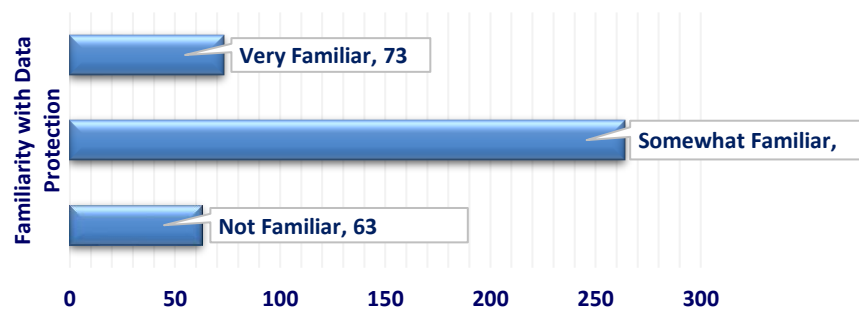


Fig. 6.3 Familiarity with term Data Protection

Table 6.4: Familiarity across Age Groups

	18-25	26-35	36-45	46-60	Total
<i>Not Familiar</i>	56	5	2	0	63
<i>Somewhat Familiar</i>	212	37	12	3	264
<i>Very Familiar</i>	42	17	13	1	73
Total	310	59	27	4	400

The data reveals that awareness of the term “data protection” varies across age groups, with younger respondents showing higher familiarity. Among the 18-5 age group, a majority (212 respondents) reported being somewhat familiar, while 42 respondents reported being very familiar. Awareness decreases with age, as only 17 respondents aged 26-35 and 13 (36-45) reported being very familiar, and minimal familiarity was observed among those aged 46-60.

To gain a deeper understanding of the respondents’ familiarity with data privacy and level of awareness, the following questions were asked. These questions aimed to assess the depth of public awareness and understanding of digital rights.

Q1. Have you heard of the Digital Personal Data Protection Act 2023?

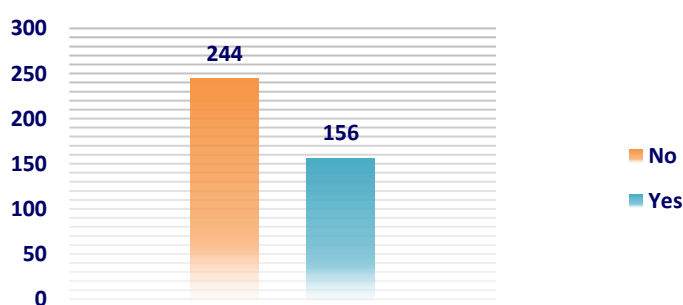


Fig: 6.4 Awareness about DPDP Act

The first question sought to assess whether respondents had heard of the Digital Personal Data Protection Act 2023. Out of 400 respondents, 244 (61%) reported that they had *not heard*, while 156 (39%) stated they had *heard of it*. This data reveals a moderate awareness deficit among the population. Despite the DPDP’s nationwide

significance, its visibility and dissemination in Nagaland remain limited. The fact that nearly two-thirds of respondents had no prior knowledge of the Act underscores the communication gap between national policy and peripheral regions. These findings align with the earlier observation that most respondents were only “*somewhat familiar*” with the term data protection

Q2. Have you ever read any documents or articles related to data protection laws in India?

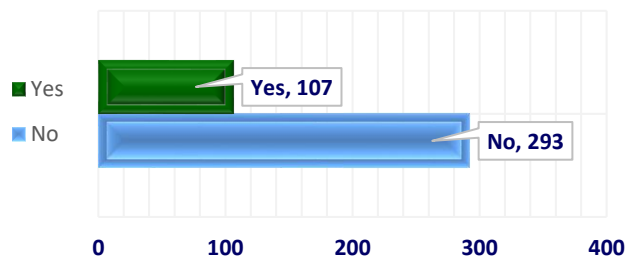


Fig 6.5 Read about Data Protection

The second question examines whether respondents had ever read any documents or articles related to data protection. Out of 400 respondents, 293 (73.3%) reported *no* and 107 (26.7%) of respondents *had read about it*. These findings complement the earlier data on familiarity with data protection. Most individuals are aware of the concept but lack depth of understanding regarding their rights or seeking redress.

Q3. Have you seen any public awareness campaigns related to data protection in Nagaland?

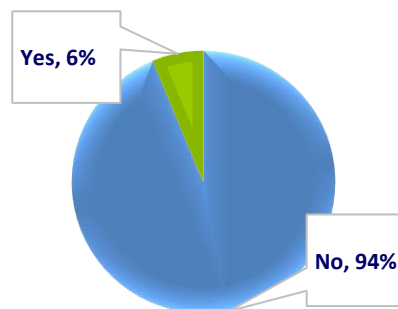


Fig 6.6 Public awareness Campaign

The third question explores whether respondents had seen any public awareness campaigns related to data protection in Nagaland. The result shows a striking lack of visibility; 375 (93.8%) reported *not having seen any such campaigns*, while only 25 respondents (6.2) affirmed *having come across*. The data highlights a critical policy communication shortfall. Despite the DPDPA’s emphasis on informed consent and public participation, there appears to be little on-ground sensitisation or outreach activity in Nagaland.

2. *Awareness about the right to privacy and the right to be forgotten*

Q4. Are you aware of the Right to Privacy as a fundamental right recognized by the Indian Constitution?

The fourth question explored whether respondents were aware that the right to privacy is recognized as a fundamental right under the Indian Constitution. The data indicate a high level of general awareness; out of 400 respondents, 356 (89%) are *aware*, while 44 (11%) were *unaware*. This pattern suggests that the right to privacy as a constitutional principle has achieved significant recognition among the general public in Nagaland.

Table 6.5: Awareness about rights

Awareness about the Right	Responses	Frequency	Percentage
<i>Are you aware of the Right to Privacy as a fundamental right recognized by the Indian Constitution?</i>	No	44	11 %
	Yes	356	89 %
	Total	400	100 %
<i>Are you aware of the Right To Be Forgotten under data protection law?</i>	No	280	70 %
	Yes	120	30 %
	Total	400	100 %

Q5. Are you aware of the Right To Be Forgotten under data protection law?

The fifth question examined awareness of the “*Right to be Forgotten*”, a critical provision in modern data regimes that allows individuals to request the erasure of their personal data under certain conditions. The responses reveal a marked decline in

awareness compared to the right to privacy. Out of 400 respondents, 280 (70%) were *unaware*, and only 120 (30%) were *aware of it*. This data reflects a significant knowledge gap regarding more technical or emerging privacy rights within India's data protection framework.

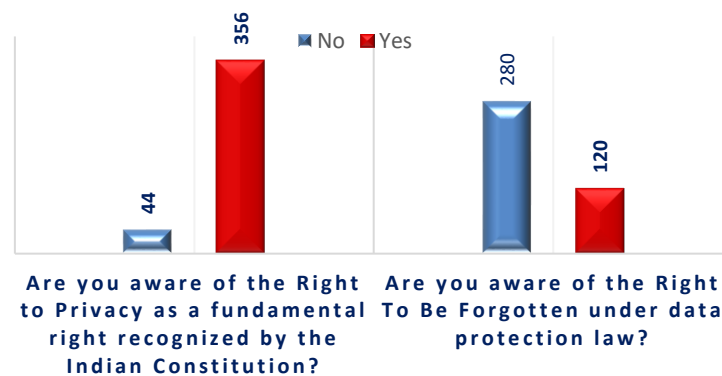


Fig 6.7 Awareness about rights

3. Individual Experience on Data Breach:

The individual experience with data breach seeks to understand the extent to which citizens in Nagaland have personally encountered incidents related to data misuse or breach of personal information. By understanding both self-reported experience and institutional insight from the Police Headquarters, the analysis provides a grounded understanding of how individuals perceive and experience digital vulnerability.

Q6. Have you ever experienced a data breach involving your personal information?

Q7. Have you encountered any data protection issues that are specific to the state of Nagaland?

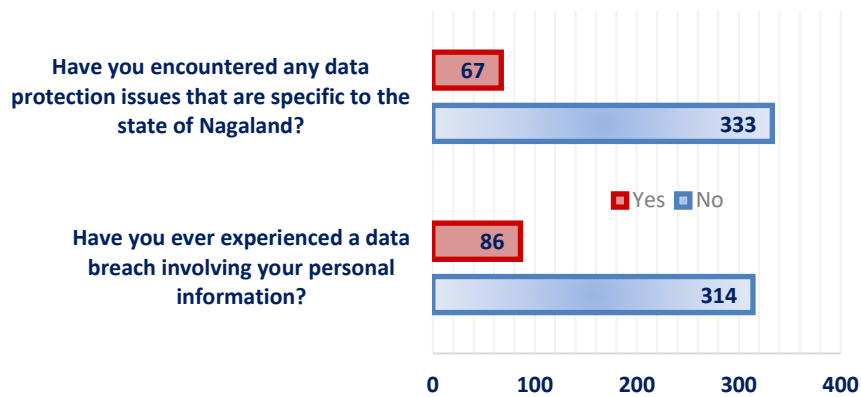


Fig 6.8: Data Breach Experience

The first question sought to determine whether respondents had ever personally experienced a data breach involving their personal data. Out of 400 respondents, 314 (78.5%) reported that they *had not experienced* any such breach, while 86 respondents (21.5%) confirmed that they *had encountered a data breach*. The second question explored whether respondents had encountered any data protection issues specific to the State of Nagaland. The result indicates that 333 (83.25%) had *not encountered* such issues, while 67 respondents (16.75%) reported that they had *faced challenges*.

Table 6.6: Data Breach Experiences

Items	Responses	Frequency	Percentages
<i>Have you ever experienced a data breach involving your personal information?</i>	No	314	78.5 %
	Yes	86	21.5 %
	Total	400	100 %
<i>Have you encountered any data protection issues that are specific to the state of Nagaland?</i>	No	333	83.25 %
	Yes	67	16.75 %
	Total	400	100 %

Further, the insights from the police Headquarters provide a more detailed picture of the situation. According to the April 2025 report (42 complaints received), as of now, no specific incidents of data breach have been officially reported in Nagaland. However, various forms of online fraud have been reported, including financial fraud

(12 cases), investment scam (6 cases), loan scams (5 cases), **impersonation (4 cases)**, Instagram-related fraud (4 cases), online gaming scams (3 cases), Facebook fraud (3 cases), wrong transaction (2 cases), Telegram fraud (2 cases) and Job scam 1 cases. The interview with officials from the Police Headquarters further clarifies that, to date, no formal incident of data breaches has been recorded in the State. The individuals who reported having experience with data-related issues, in most cases, were victims of various forms of cyber fraud and social media scams. While data breaches in the strict legal sense remain rare in Nagaland, misuse of personal information is emerging as a pressing concern.

4. Public Perception on Emerging Technologies

To complement the broader inquiry into people's understanding of data privacy and protection, a set of questions was designed to explore citizens' perceptions of emerging technologies and their implications for personal data security. Understanding these perceptions helps reveal how individuals in Nagaland relate technological innovation to privacy, trust and legal protection. These questions are:

Q8. Do you believe emerging technologies (AI, IoT) pose a greater risk to personal data privacy?

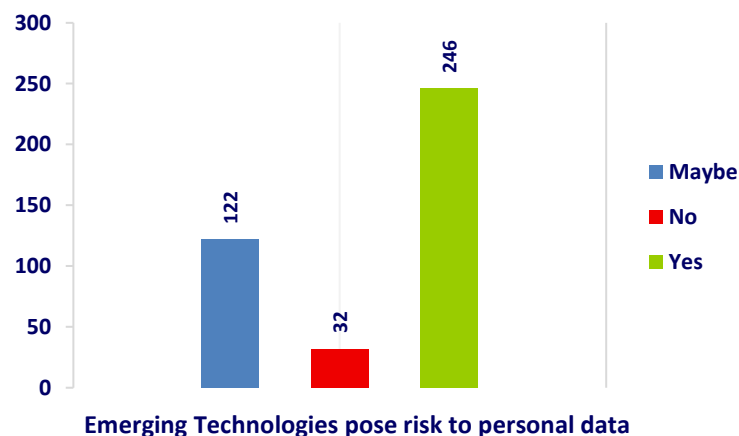


Fig 6.9: Perception about technologies

Q.9 Do u believe that technological advancements like encryption can mitigate data privacy risks?

Q 10. Should new technologies like AI and machine learning be regulated under data protection laws?

In response to the question “Do you believe emerging technologies (AI, IoT) pose a greater risk to personal data privacy?” 246 (61.5%) answered *Yes*, while 122 (30.5%) respondents indicated *Maybe*, and only 32 (8%) said *No*. The second question explored whether respondents believe that technological advancements such as encryption can help mitigate data privacy risks. Here, opinions were more divided: 203 respondents (50.75%) answered *Yes*, 161 respondents (40.25%) said *Maybe*, and 36 respondents (9%) said *No*.

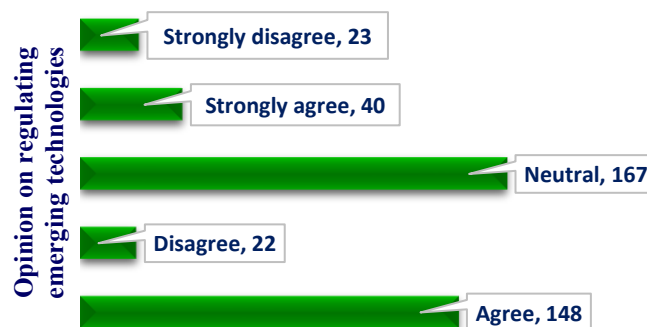


Fig 6.10: Public opinion on regulation of emerging technologies

The third question assesses public opinion on whether AI and machine learning should be regulated under data protection laws. The responses indicate 148 respondents (37%) *agreed*, 40 (10%) *strongly agreed*, 167 (41.8%) remained *neutral*, 22 (5.5%) *disagreed*, and 23 (5.8%) *strongly disagreed*. The responses reveal both awareness and uncertainty that could shape the effective implementation of data protection laws in Nagaland. While a majority (61.5%) recognizes the *risk posed by emerging technologies*, the higher proportion of “*may be*” responses suggests limited technical understanding of how such risks operate. Although most respondents support the

regulation of AI and ML, widespread neutrality shows a cautious optimism rather than informed conviction. These mixed perceptions highlight the need for digital literacy and public sensitisation to strengthen compliance with data protection laws in Nagaland.

5. Privacy Practices by Individuals

To understand how individuals in Nagaland practice data security in their daily digital activities to safeguard their personal data, respondents were asked about two key behavioural aspects (the responses are present in Figures 6.12 and 6.13):

Q.11 How often do you change your passwords or take steps to protect your personal information online?

Q12. How often do you change your passwords or take steps to protect your personal information online?

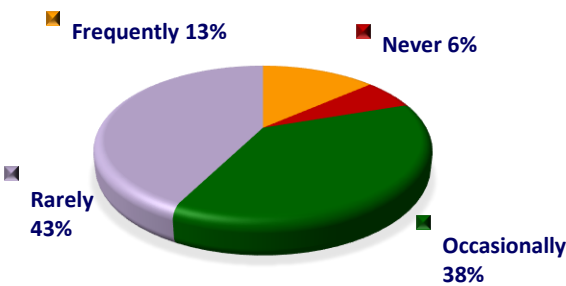


Fig 6.11 Frequency of Password Change

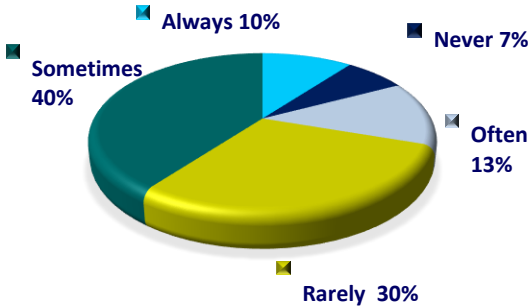


Fig 6.12: Frequency of Website policy checking

The data shows that online security and privacy practices among respondents are relatively low and inconsistent. Regarding password management, only 13.5% of the respondents change their passwords, while 37.8% do so occasionally and 42.5% rarely take such actions. This suggests a general lack of proactive behaviour towards safeguarding personal information online. Similarly, for the second question, only 10.3% of respondents *always check* the privacy policies of websites or applications

before use, while a combined 69.8% either check them *rarely or only sometimes*. This pattern highlights a tendency towards complacency and a lack of habitual awareness of privacy in online interactions. These findings reveal that while awareness of data privacy may exist at a conceptual level, it has not yet translated into consistent protective behaviour among users in Nagaland.

4 HYPOTHESE TESTING

The hypotheses proposed in this study have been systematically examined through the doctrinal, analytical and empirical discussions presented in this chapter. Each hypothesis has been assessed in light of the analytical insights and empirical findings gathered throughout the study. The status of each hypothesis, whether validated, partially upheld or refuted, is presented in a structured way as follows:

Hypothesis 1: *The current legal framework governing data protection in India ensures the protection of personal data and the privacy rights of citizens in all states, including Nagaland.*

India's data protection landscape is anchored primarily in the Information Technology Act 2000, IT Rule 2011, sectoral regulations and ongoing reforms to the Digital Personal Data Protection Act 2023. The examination of this hypothesis is conducted through a close assessment of the normative, constitutional, and territorial reach of India's data protection regime, particularly the Digital Personal Data Protection Act 2023, and its applicability to the unique constitutional and socio-legal setting of Nagaland. To begin with, the constitutional competence of Parliament to legislate in the domain of data protection is unequivocally established. The framers of the Constitution could not have foreseen the complexities of digital data, leading to the absence of explicit references to data governance within the Seventh Schedule. As a result, matters about digital data, privacy, and information flows fall within Parliament's residuary legislative authority under Article 248, read with Entry 97 of the Union List. Additionally, aspects of electronic communication and data transmission are already subsumed under Entry 31 of the Union List. Therefore, the

DPDP Act 2023 stands on firm constitutional ground as a valid central legislation applicable uniformly across India, including the state of Nagaland.

Secondly, the jurisdictional scope of the DPDP Act 2023, as articulated under section 3 governs all personal data processed within India, regardless of whether it was originally collected in digital or non-digital form. It also possesses extraterritorial jurisdiction when foreign entities process data relating to individuals located in India. Consequently, the law binds all categories of actors operating within Nagaland's state agencies, local bodies, private enterprises, financial institutions, and even community institutions, provided they engage in digital processing. International platforms serving residents of Nagaland are equally bound by the Act. Thus, from a jurisdictional standpoint, the law's coverage is sufficiently comprehensive.

Thirdly, the analysis is Nagaland's special constitutional status under Article 371(A). This article safeguards Naga customary practices, religious and social traditions, the administration of justice based on local customs, and ownership and transfer of land and its resources. However, digital personal data protection does not fall within these protected domains. The DPDP Act regulates technological and administrative processes related to privacy, data governance, and accountability of matters that fall outside the scope of customary laws and traditional institutions. As such, the applicability of the Act in Nagaland does not require a resolution of the State Legislative Assembly. There is no constitutional incompatibility or encroachment upon Article 371(A).

Lastly, the insights gathered during the interview with the District Commissioner offer clarity on the jurisdictional boundaries between Nagaland's traditional institutions, particularly the Dobashi Courts and the national framework governing data privacy. The Dobashi Courts, as reaffirmed in the discussion, continue to function primarily as customary civil dispute resolution bodies dealing with matters rooted in local customary practices. They do not possess the institutional mandates, procedural infrastructure, or statutory authority to address concerns relating to personal data protection or digital privacy. Conversely, issues surrounding the safeguarding of

personal data, digital rights and data privacy fall squarely within the purview of India's central legal frameworks, which include the Information Technology Act, accompanying Rules, and most significantly the Digital Personal Data Protection Act 2023. These laws are structured to operate uniformly across all states and union territories, ensuring that citizens, irrespective of local administrative or customary systems, remain protected under a consistent data governance framework. Thus, customary forums like Dobashi Courts continue to play an important role in Nagaland's unique administrative system, and the protection of personal data remains exclusively governed by central legislation, which overrides any local or traditional mechanisms in matters related to digital governance.

Taken together, these constitutional, jurisdictional, and contextual findings demonstrate that India's data protection framework does indeed apply fully and effectively to the State of Nagaland. Taken together, these findings validate the core assumption underlying Hypothesis 1. The legal framework governing data protection in India is constitutionally sound, legislatively competent, territorially comprehensive, and fully applicable to Nagaland. Thus, the hypothesis "*the current legal framework governing data protection in India ensures the protection of personal data and the privacy rights of citizens in all states, including Nagaland*" **stands validated.**

Hypothesis 2: *The enforcement and implementation of the DPDP Act 2023 in the State of Nagaland face significant administrative, infrastructural and institutional challenges due to limited digital readiness and data governance constraints.*

To test this hypothesis, the study adopts an integrated approach that examines how administrative, infrastructural and institutional limitations shape the implementation of the DPDP Act 2023 in Nagaland. Administratively, the focus is on assessing government readiness, the availability of trained staff and the capacity of organizations to comply with new data protection obligations. Infrastructural aspects are explored by considering the state's internet penetration, digital literacy, and technological gaps that may hinder compliance. Institutional challenges are analyzed

by evaluating how organizations manage personal data, implement security practices and communicate privacy policies to users. The doctrinal insights are complemented by a robust set of survey questions designed to capture citizen awareness, experience with digital services, and views on governance structure. Together, these elements create a comprehensive framework for understanding whether Nagaland is adequately prepared for effective enforcement of the Digital Personal Data Protection Act 2023.

i. Administrative Challenges:

The administrative capacity of the government institution in Nagaland remains one of the central determinants in assessing the state's readiness to implement the DPDP Act 2023. Despite ongoing national efforts towards strengthening digital governance, Nagaland continues to rely extensively on manual, paper-based administrative processes. This structural reliance significantly limits the state's ability to adopt the digitalized workflows required for compliance with the Act. This challenge is further amplified by an important regulatory fact, the Digital Personal Data Protection Rule 2025, which is expected to serve as the operational backbone of the DPDP Act by prescribing detailed procedures, technical standards, and compliance timelines that have not yet come into force. These Rules are intended to act as "*working machinery*" of the Act, clarifying obligations for government institutions, specifying security requirements, and establishing a reporting framework. Their absence creates additional ambiguity for a state like Nagaland, where administrative readiness is already constrained. Without the Rules being implemented, departments lack clarity on procedural expectations, capacity-building requirements, and technical specifications, making compliance planning even more difficult. The administrative shortcomings directly affect the State's ability to fulfil core legal mandates of the Act, such as:

- Issuing compliant notice and consent frameworks,
- Establishing accessibility grievance redressal mechanisms,
- Conducting periodic data audits,
- Maintaining secure data storage and retention systems, and
- Enabling timely data breach reporting to the central authorities.

ii. Infrastructural Challenges:

Infrastructural constraints constitute a major barrier to the effective implementation of the Digital Personal Data Protection Act 2023 in Nagaland. Despite gradual improvements in digital connectivity across the northeastern region, Nagaland's foundational digital infrastructure remains comparatively underdeveloped and unevenly distributed, especially between urban and rural remote regions. The digital preparedness of institutions themselves is another limitation. Many government offices, small and medium enterprises and service providers operate with outdated computer systems, insufficient storage capacity, and minimal cybersecurity safeguards. The absence of secure servers and updated operating systems significantly restricts their ability to store personal data safely, maintain consent logs, or respond effectively to potential data breaches. These infrastructural impediments restrict not only the operational feasibility of the DPDP Act but also citizens' ability to meaningfully exercise their digital rights.

iii. Institutional Challenges:

Institutional readiness represents another critical dimension shaping the feasibility of implementing the DPDP Act 2023 in Nagaland. While the Act prescribes clear obligations for both public and private entities, the institutional landscape in the state is still at an early stage of developing the systems and practices necessary to support a comprehensive data protection regime. The low level of institutional awareness regarding legal responsibilities and liabilities associated with data breaches. In several departments and private entities, unfamiliar with statutory duties related to breach reporting, grievance handling and record keeping. To understand the institutional challenges associated with data protection, two questions were asked of the respondents: (1) *How would you rate the effectiveness of data protection measures in your workplace on a scale of 1-5? (Scale 1 is “very ineffective”, to 5 is “very effective”)* and (2) *In your opinion, which sector requires the most attention regarding data protection laws?.* The responses provide valuable insights into the perceived adequacy of institutional data protection mechanisms, and which sector requires more

attention for stronger data protection policies. The distribution of responses (Figure 6.13) reflects a clear pattern of moderate but inadequate institutional preparedness. Rating 1-3 (82.8%) of respondents believe their workplace has only moderate, weak, or very weak data protection measures. Rating 4-5, (27.3%) view them as effective or highly effective. Whereas the concentration of rating 3 (56%) suggests that most organizations have basic, incomplete or inconsistent data protection practices.

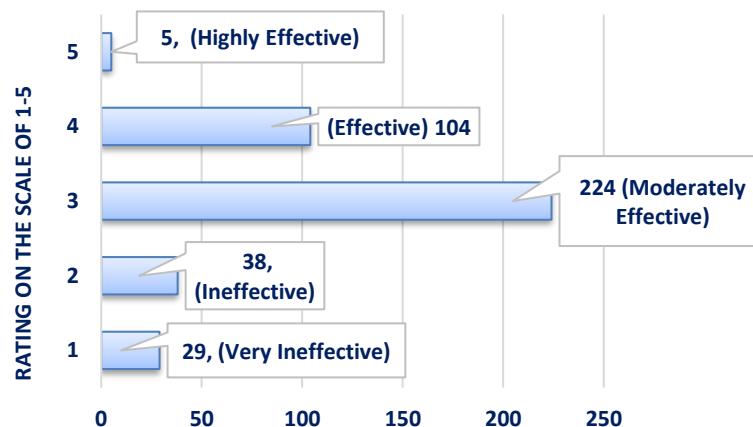


Fig. 6.13: Data Privacy at Workplace

In response to the second question, 60.8% of the respondents identified the “*banking*” sector as requiring the most attention regarding data protection laws. This is followed by “*healthcare*” (12.8%) and “*government services*” (11%). These results underline the sectors that citizens perceive as most vulnerable due to the sensitive nature of financial and health data handled daily.

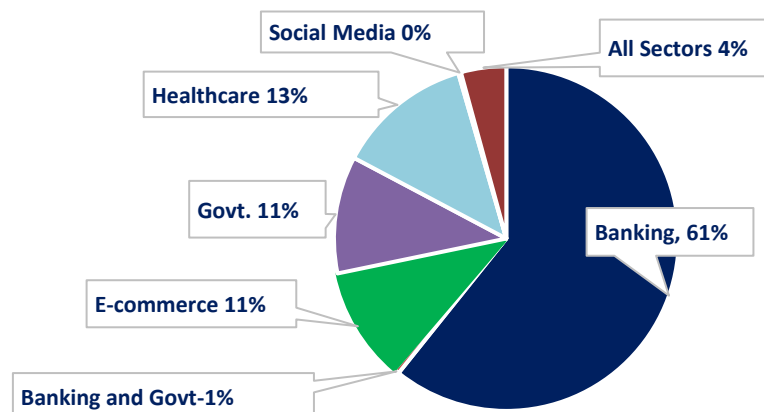


Fig 6.14: Which sector require more attention

iv. Public Perceptions of Digital Governance and Privacy Compliance in Nagaland:

The empirical part of this study focuses on exploring how individuals in Nagaland experience and perceive organizational transparency, data usage practices, and accountability mechanisms. With the doctrinal analysis highlighting administrative, infrastructural, and institutional limitations, this empirical section complements it by examining ground-level realities through survey responses. The survey questions are:

- *Have you encountered any organization providing you with information on how your data is used?*
- *Do you think organizations in India are transparent about their data protection practices?*
- *Should companies be required to inform customers immediately in case of a data breach?*

Table 6.8: Organizational transparency practice

Items	Responses	Frequency	Percentage
<i>Have you encountered any organization providing you with information on how your data is used?</i>	Yes	10	2.5 %
	No	390	97.5 %
	Total	400	100 %
<i>Do you think organizations in India are transparent about their data protection practices?</i>	Maybe	203	50.8 %
	No	138	34.5 %
	Yes	59	14.8 %
	Total	400	100 %
<i>Should companies be required to inform customers immediately in case of a data breach?</i>	No	31	7.8 %
	Only in certain cases	36	9.0 %
	Yes	333	83.3 %
	Total	400	100 %

Have you encountered any organization providing you with information on how your data is used? [97.5% respondents answered No, and only 2.5% Yes] -

This extremely high percentage of respondents who have never received information about how their data is used reveals a significant institutional weakness in data

governance practices across Nagaland. Under the DPDP Act, organizations are legally obligated to provide clear notice to data collection, the purpose of use and user rights. Yet the data indicate that this legal norm has not been translated into practice on the ground. This gap strongly reinforces Hypothesis 2, as it highlights that institutions in the state lack the administrative capacity, internal protocols and technological systems required to carry out basic compliance functions.

Do you think organizations in India are transparent about their data protection practices? [Maybe 50.8%, No 34.5% and Yes 14.8%]-

The responses to this question reveal widespread uncertainty and skepticism regarding organizational transparency. With more than half of the respondents expressing “maybe” and over one-third stating outright that organizations are “*not transparent*”, this highlights a disconnect between legal expectations under DPDP and everyday user experiences. Only 14.8% responses “yes” demonstrate that only a small fraction of the population sees that organizations are transparent. This ambiguity directly reflects the absence of accessible communication mechanisms, limited public awareness and weak institutional engagement with data rights conditions that are consistent with administrative and infrastructural barriers identified in Hypothesis 2.

Should companies be required to inform customers immediately in case of a data breach? [Yes 83.3%, Only in certain cases 9% and No 7.8%]-

The overwhelming support for mandatory and immediate breach notification demonstrates that citizens clearly value accountability and expect stronger organizational responsibility in handling personal data. These expectations, however, sharply contrast with institutional and administrative realities highlighted by the previous responses. While the public sees breach notification as essential, many institutions in Nagaland lack an incident reporting mechanism, digital infrastructure to detect, investigate and communicate breaches. Moreover, the fact that 9% believe notification should occur “only in certain cases” possibly reflects a gap in awareness of legal standards, further highlighting the need for better public awareness. This disjuncture between citizens' expectations and institutional preparedness directly

supports the hypothesis by illustrating how governance constraints and limits digital maturity hinder the ability to enforce provisions of the DPDP Act.

The findings **strongly validate the hypothesis** “*The enforcement and implementation of the DPDP Act 2023 in the State of Nagaland face significant administrative, infrastructural and institutional challenges due to limited digital readiness and data governance constraints*”. The doctrinal analysis shows clear administrative, infrastructural and institutional limitations that hinder Nagaland’s readiness to implement the DPDP Act 2023. These challenges are further reinforced by empirical evidence, 97.5% of respondents have never received information on how their data is being used by the organizations, and citizens widely expect mandatory data breach notifications. Together, these insights reveal significant gaps in digital readiness, data governance practices, and institutional capacity.

Hypothesis 3: *Awareness of the Digital Personal Data Protection Act 2023, among the citizens in Nagaland, does not differ significantly across age groups.*

This hypothesis seeks to determine whether awareness of the Digital Personal Data Protection Act 2023 is evenly distributed across age groups in Nagaland or whether generational differences influence the level of understanding and exposure to data protection laws. Awareness is not limited to merely knowing the Act exists; it also involves understanding its purpose and its contextual relevance. To achieve this objective, the following dimensions were selected to reflect the multidimensional nature of legal and policy awareness in the context of data protection

- i. Basic awareness of the DPPD Act 2023
- ii. Nagaland Context Awareness
- iii. Digital Readiness Awareness
- iv. Data Protection in Online Services
- v. Data Governance Awareness

1. Basic awareness of the DPDP Act 2023:

Q1. Do you believe the Digital Personal Data Protection Act 2023 adequately addresses data protection issues?

Table 6.9: DPDPA Adequately Addresses Data Protection Issues

Responses	Frequency	Percentage
Needs improvement	236	59.0 %
No	61	15.3 %
Yes	103	25.8 %
Total	400	100 %

The key observations from the frequency table 6.9 show that a majority of respondents 59% feel the Act needs improvement, indicating moderate or incomplete awareness. Only 25.8% believe the Act adequately address data protection issues. This distribution suggests that awareness is not uniformly strong, but the question of whether this varies across the age groups is presented in Table 6.10.

Table 6.10: Adequacy opinion Across Age Groups

Responses	18-25	26-35	36-45	46-60	Total
Needs improvement	176	40	17	3	236
No	42	13	5	1	61
Yes	92	6	5	0	103
Total	310	59	27	4	400

The crosstab shows the key patterns across the age group 18-25, which shows the strongest awareness, the largest portion answering “yes” or “needs improvement”. The older age group, 36- 60, shows lower awareness, with almost no respondents selecting “yes”. While the crosstab highlights how responses are distributed, it does not by itself confirm whether age actually influences awareness of the DPPD Act 2023. Table 6.11 presents the Chi-square test results.

Table 6.11 Relationship Between Age and Awareness (Chi-square test results)

Test	χ^2 value	df	p- value
Pearson Chi-Square	13.084	6	0.042
Likelihood Ratio	15.466	6	0.017

Interpretation:

The p-value (0.042) is less than the significance level of 0.05, indicating a statistically significant association between age and awareness. This suggests that awareness varies across different age groups. The likelihood ratio test ($p = 0.017$) further supports these findings, confirming that awareness is not independent of age.

Result:

The analysis of the awareness dimension using Q1 indicates that perceptions of the DPDPA vary across age groups. The Chi-Square Test reveals a statistically significant association between age and awareness $\chi^2(6) = 13.084, p = .042$. The cross-tabulation further indicates that younger respondents display a higher level of engagement and awareness compared to older groups, who have limited familiarity. These findings collectively demonstrate that awareness of the DPDP Act is not uniform across age groups. Therefore, the hypothesis stating *that awareness does not differ significantly across age groups* **is not supported by the data for this dimension**.

2. Nagaland Context Awareness:

Q2. Do you think data protection laws need to be modified to suit the specific needs of Nagaland?

To examine whether perceptions about modifying data protection laws for Nagaland vary across demographic groups, a cross-tabulation was first conducted to observe how responses differed among participants. While crosstab results reveal distribution patterns, they do not confirm whether these differences are significant. Therefore, a chi-square test was applied to statistically assess the relationship between respondents'

age categories and their views. This combined approach helps determine whether the hypothesis is supported by empirical evidence.

Table 6.12: Data protection laws need to be modified

Responses	18-25	26-35	36-45	46-60	Total
No	143	23	14	0	180
Yes	167	36	13	4	220
Total	310	59	27	4	400

The data shows that all age groups show a similar number of respondents who say “yes” than “no”. The proportions across age groups do not differ sharply. Even older groups show agreement with modifications.

Table 6.13: Chi-Square Test Results

Test	χ^2 value	Df	p-value
Pearson Chi-Square	4.808	3	0.186
Likelihood Ratio	6.324	3	0.097

Interpretation:

The p-value = 0.186 > 0.05 for Pearson is not significant, and p = 0.097 for Likelihood Ratio is not significant, though closer to significance. Since both p-values are greater than 0.05, this indicates that there is no statistically significant association between the age group and responses to question 2. Age does not significantly affect how people perceive Nagaland’s unique data protection needs.

Result:

Analysis of question 2, which measures respondents' awareness of the need to modify the data protection laws to Nagaland’s specific context, shows no significant variation across age groups. The Chi-Square test shows a non-significant result, χ^2 (3, N= 400) = 4.81, p = .186 supported by the non-significant likelihood ratio (p = .097). The

distribution of responses “yes” and “no” was proportionately similar across all age categories, indicating that awareness of Nagaland-specific modification to the DPDP Act is uniformly shared. Thus, **the findings support the Hypothesis** for this dimension, confirming that awareness does not differ significantly across age groups.

Q3. Should Nagaland create its own data protection policies to complement national laws?

To assess whether perceptions about state-specific data protection policies vary across age groups, the question “*Should Nagaland create its own data protection policies to complement national laws?*” was first examined through descriptive analysis (Table 6.14) to observe overall response patterns. Further, the K-Test (6.16) was applied to determine whether these differences were statistically significant.

Table 6.14: Should Nagaland create its own data protection policies

	Responses	Frequency	Percentage
<i>Should Nagaland create its own data protection policies to complement national laws?</i>	Strongly Disagree	18	4.5 %
	Disagree	19	4.8 %
	Neutral	55	13.8 %
	Agree	193	48.3 %
	Strongly Agree	115	28.8 %
	Total	400	100 %

The distribution of responses shows a strong overall endorsement for creating Nagaland-specific data protection policies. Nearly half of the respondents, 48.3%, agree, and 28.8% strongly agree, indicating that over 77% support region-specific data protection measures. Only a very small share, 4.5% strongly disagree, and 4.8% disagree. Only 13.8% remain neutral. The results reflect a clear public preference for policies tailored to Nagaland's unique socio-legal context.

Table 6.15: Descriptive Analysis (Mean Rank)

Age Group	N	Mean Rank
18-25	310	204.55
26-35	58	191.35
36-45	28	180.63
46-60	4	158.00

Interpretation:

Mean ranks decrease gradually with age. Younger groups generally agree more strongly that Nagaland should create its own policies. The differences in mean rank alone do not confirm a statistically significant. Further K-Test was performed, the results are presented in Table 6.16

Table 6.16: Kruskal-Wallis Test Results

Statistics	Value
Kruskal-Wallis H	2.453
df	3
p-value	0.484

Interpretation:

The value of $p = 0.484 > 0.05$, which means awareness is uniform across age groups. Age does not significantly influence the opinions on this issue. Even though the mean ranks suggest a pattern, the differences are not statistically significant.

Result:

The Kruskal-Wallis test was conducted to assess whether age groups differed in their views regarding the need for Nagaland to create its own data protection policies to complement national legislation. The results revealed no significant variation across age categories ($h = 2.453$, $df = 3$, $p = .484$). Although mean ranks showed a slight decline with increasing age, these differences were not statistically meaningful. This

demonstrates that awareness within this dimension is uniform across age groups, **thereby validating Hypothesis 3** for this question.

3. Digital Readiness Awareness:

Q4. Are you confident in the current cybersecurity infrastructure in India?

To examine whether awareness of national cybersecurity readiness varies across age groups in Nagaland, descriptive analysis (Table 6.17) and Chi-Square Test (Table 6.18) were applied to responses for Q4. This item forms part of the Digital Readiness Awareness dimension, which assesses citizens' understanding of the technological capacity underpinning the DPDP Act 2023. The descriptive analysis provides an overview of public opinion, and the Chi-Square test evaluates whether differences in perceptions are statistically significant across age categories.

Table 6.17: Citizens' Perceptions on Digital Infrastructure

	Responses	Frequency	Percentage
<i>Are you confident in the current cybersecurity infrastructure in India?</i>	Needs improvement	183	45.8 %
	No	123	30.8 %
	Yes	94	23.5 %
	Total	400	100 %

The descriptive data (Table 6.17) reveal how respondents evaluate India's cybersecurity infrastructure. A substantial portion, 45.8%, responded “*needs improvement*”, showing that nearly half of the population believes that the national cybersecurity ecosystem requires strengthening. 30.8% responded “no”, and 23.5% reported confidence in the cybersecurity infrastructure. This distribution highlights a general tendency towards skepticism regarding India's preparedness to protect digital data effectively. Patterns across age groups look somewhat similar; each group shows the same ranking **needs improvement > no > yes**.

Table 618: Chi-Square Test Result of Digital Infrastructure across age groups

Test	χ^2 value	Df	p-value
Pearson Chi-Square	10.488	6	0.106
Likelihood Ratio	11.324	6	0.079

Interpretation:

The value of $p = .106$ (Pearson) and $p = .079$ (Likelihood Ratio), both values are greater than 0.05, which means that no significant association exists between age group and confidence in cybersecurity infrastructure. Awareness in this dimension is not significantly different across age groups.

Result:

The Pearson Chi-Square statistic $\chi^2 = 10.88$, $df = 6$ and $p = 0.106$ is not statistically significant as the p -value exceeds the 0.05 threshold. This shows that the distribution of confidence level does not differ significantly across age groups. Thus, the statistical evidence shows that respondents across different age groups express similar levels of confidence, concerns and perceived need for improvement. Therefore, the findings substantiate Hypothesis 3 for this dimension: **age does not significantly influence awareness** relating to national cybersecurity infrastructure.

Q5. Do you think internet access and digital literacy affect the implementation of data protection laws?

To assess whether perceptions of infrastructural factors vary across age groups, the question “*Do you think internet access and digital literacy affect the implementation of data protection laws?*” was examined through descriptive analysis and the Chi-Square Test of Independence. This item forms part of the digital readiness awareness dimension, which evaluates citizens’ understanding of technology and literacy-based preconditions necessary for effective implementation of the Digital Personal Data Protection Act 2023. The Descriptive analysis (Table 6.19) findings overview of

public opinion, while the Chi-Square Test (Table 6.20) determine whether these views differ significantly across age groups.

Table 6.19: Public Opinion on Digital Literacy

Item	Responses	Frequency	Percentage
<i>Do you think internet access and digital literacy affect the implementation of data protection laws?</i>	No	88	22 %
	Yes	312	78 %
	Total	400	100 %

The descriptive findings reveal that a substantive majority of respondents 78% believe that internet access and digital literacy directly influence the implementation of data protection laws in Nagaland. Only 22% responded “no,” suggesting a relatively small segment of the population does not link access and literacy with data governance effectively. Overall, the descriptive results highlight a generally well-informed public understanding of the infrastructural factors necessary for effective data protection implementation.

Table 6.20: Chi-Square Test result

Test	χ^2 value	Df	p-value
Pearson Chi-Square	8.558	3	0.036
Likelihood Ratio	10.335	3	0.016

Interpretation:

The Pearson value of $p = 0.036 < 0.05$ and the Likelihood Ratio $p = .016 < 0.05$ show a significant association between age group and responses. Younger respondents show greater awareness, and older groups show limited recognition of infrastructural barriers.

Result:

The Chi-Square Test of Independence was used to determine whether perceptions differed significantly across age groups. The Pearson Chi-Square value ($\chi^2 = 8.558$,

df = 3) shows a significant p-value of 0.036, indicating that age is statistically associated with respondents' views. This means that younger respondents are more likely to acknowledge the role of digital access and literacy, whereas older groups display comparatively lower awareness. Therefore, Hypothesis 3 is not supported by the data for the Digital Readiness Awareness dimension measured through Q5: **the evidence does not support Hypothesis** for this dimension, as awareness regarding these infrastructural factors varies with age.

Q6. Should Nagaland invest in digital infrastructure to support data protection laws?

To examine whether awareness of infrastructural requirements for effective data protection varies across age groups, the question “*Should Nagaland invest in digital infrastructure to support data protection laws?*” was analyzed using descriptive statistics and the Chi-Square test of Independence. This item reflects the Digital Readiness Awareness dimension, which assesses respondents' understanding of the technological foundations necessary for the successful implementation of the Digital Personal Data Protection Act. Descriptive analysis (Table 6.21) shows the frequency of responses, and the Crosstab (Table 6.22) and Chi-Square test (Table 6.23) evaluate whether these views differ significantly across age groups.

Table 6.21: Descriptive Analysis for Nagaland Digital Infrastructure

Item	Responses	Frequency	Percentage
<i>Should Nagaland invest in digital infrastructure to support data protection laws?</i>	Maybe	96	24 %
	No	20	5 %
	Yes	284	71 %
	Total	400	100 %

The descriptive results indicate strong public support for the view that Nagaland should invest in digital infrastructure to strengthen data protection measures. A substantial majority of respondents 71% answered “yes”, demonstrating clear recognition of the importance of technological foundations for implementing the DPPD Act. Whereas 2% selected “maybe”, suggesting moderate agreement or

uncertainty, while only 5% responded “no”, indicating minimal opposition. This shows a high level of awareness among citizens regarding the significance of digital infrastructure in enhancing data protection compliance.

Table 6.22: Age group x Support for Digital Infrastructure (Cross-tabulation)

Responses	18-25	26-35	36-45	46-60	Total
Maybe	79	11	4	2	96
No	18	2	0	0	20
Yes	213	46	23	2	284
Total	310	59	27	4	400

The crosstabulation shows a strong endorsement for investing in digital infrastructure across all age groups, with 284 respondents 71% agreeing that such investment is necessary for effective data protection law implementation. Age group 18-25 (213 respondents) selected “yes”, indicating a digitally aware younger population. The 26-35 and 36-5 group show substantial support. A very few respondents across any age category responded “no”. The “maybe” category accounts for 96 responses, suggesting some uncertainty. The uniformity of response across all age groups, especially “yes”, indicates a broad generational consensus on the need for digital infrastructure development to strengthen data protection implementation in Nagaland.

Table 6.23: Chi-Square Independent Test Result

Test	χ^2 value	df	p-value
Pearson Chi-Square	6.970	6	.324
Likelihood Ratio	8.447	6	.207

Interpretation:

The Chi-Square test results show $p = 0.324$, which is greater than 0.05; the test is not statistically significant. This means that there is no meaningful relationship between age group and support for digital infrastructure to strengthen data protection laws.

Result:

The Chi-Square Test of Independence was applied to determine whether the level of support for infrastructure investment differed across age groups. The Pearson Chi-Square result $\chi^2 = 6.970$, $df = 6$, $p = 0.324$ was not statistically significant, showing no association between age and response patterns. The analysis demonstrates that awareness of the role of digital infrastructure in supporting data protection laws does not vary significantly across age groups. **Hypothesis 3 is validated** for Q6, indicating that the need for digital infrastructure investment does not differ significantly across age categories.

4. Personal Data Protection Awareness:

Q7. Do you believe your data is adequately protected when you use online services?

To understand whether perceptions of online data safety differ across age groups, the question “*Do you believe your data is adequately protected when you use online services?*” was analyzed using descriptive statistics and the Chi-Square Test of Independence. This question falls under the Personal Data Protection Awareness dimension, which captures citizens’ confidence in the security of their personal information in the digital ecosystem. The descriptive analysis (Table 6.24) establishes a pattern of responses, while the Chi-Square test (Table 6.26) examines whether these perceptions vary significantly across age groups.

Table 6.24: Data Protected over Online Service

Item	Responses	Frequency	Percentages
<i>Do you believe your data is adequately protected when you use online services?</i>	No	229	57.3 %
	Yes	171	42.8 %
	Total	400	100 %

The descriptive findings show that a slight majority of respondents, 57.3%, do not believe their data is adequately protected when using online services, indicating a

general sense of vulnerability and skepticism regarding online data security. Meanwhile, 42.8% expressed confidence in the protection of their data. This distribution highlights a moderate divide in public perceptions, with more respondents leaning towards concerns about data safety.

Table 6.25: Data on Online Services across age groups

Responses	18-25	26-35	36-45	46-60	Total
No	174	37	15	3	229
Yes	136	22	12	1	171
Total	310	59	27	4	400

When analyzed across age groups through crosstabulation, similar patterns emerge; all age groups show more “no” responses than “yes”, suggesting a shared skepticism. To determine whether these differences are statistically significant, a Chi-Square test of Independence was applied.

Table 6.26: Chi-Square Test Result (Online Data Safety)

Test	χ^2 value	df	p-value
Pearson Chi-Square	1.425	3	.700
Likelihood Ratio	1.466	3	.690

Interpretation:

The Pearson value of $p = .700$ and Likelihood Ratio $p = .690$; both p-values are far greater than 0.05, which means that there is no statistically significant association between age group and belief that data is adequately protected when using online services. Thus, confidence in online data protection does not differ significantly across age groups.

Result:

The Pearson Chi-Square statistics $\chi^2 = 1.425$, $df = 3$, $p = 0.700$ indicates no significant association between age group and perception of data safety. The results demonstrate

that age does not influence perception of online data safety. Since no statistically significant difference was found ($p > 0.05$), **Hypothesis 3 is validated for this dimension**. This means that awareness about personal data safety does not differ significantly based on age.

5. Data Governance Awareness:

Q8. Do you think data localization will improve the security of Indian citizens' data?

To assess whether awareness of data governance varies across age groups, the question “*Do you think data localization will improve the security of Indian citizens' data?*” was analyzed using descriptive statistics and the Chi-Square Test of Independence. The descriptive analysis (Table 6.27) highlights overall public sentiment, while the Chi-Square test (Table 6.29) determines whether age significantly influences these perceptions, enabling evaluation of Hypothesis 3.

Table 6.27: Public Perception of Data Localization

Item	Responses	Frequency	Percentage
<i>Do you think data localization will improve the security of Indian citizens' data?</i>	Maybe	214	53.5 %
	No	26	6.5 %
	Yes	160	40 %
	Total	400	100 %

The descriptive data show that more than half of the respondents, 53.5% selected “maybe”, indicating uncertainty or moderate agreement with the security benefits of data localization. A substantial proportion 40% responded “yes” reflecting strong support, while only 6.5% expressed disagreement. This distribution suggests that most respondents believe data localization has potential security advantages or are at least open to the idea. Overall, public sentiment leans positively toward data localization as a mechanism for enhancing data protection for Indian citizens.

Table 6.28: Public Perception of Data Localization Across Age Groups

Responses	18-25	26-35	36-45	46-60	Total
Maybe	162	40	9	3	214
No	21	3	1	1	26
Yes	127	16	17	0	160
Total	310	59	27	4	400

The crosstab results show noticeable variations across age groups. Younger respondents, 18-25 show a higher frequency of “yes” and “maybe”, while older groups display mixed patterns, with very low counts in some categories. The age group 36-45 shows a stronger proportion of “yes” responses relative to its size, whereas the older age group 46-60 shows minimal participation and varied responses. These visible differences across age groups suggest that the perception of data localization benefits may not be uniform across age groups.

Table 6.29: Chi-Square Test Result (Perception of Data Localization)

Test	χ^2 value	df	p-value
Pearson Chi-Square	15.069	6	.020
Likelihood Ratio	15.738	6	.015

Interpretation:

The Pearson Chi-Square test shows $\chi^2 = 15.069$, $df = 6$, $p = .020$ and the Likelihood Ratio test shows $\chi^2 = 15.738$, $p = .015$. Both the p-values are below 0.05, indicating a statistically significant relation between age and data localization awareness.

Result:

The Chi-Square Test of Independence was conducted to determine whether perceptions of data localization differed across age groups. These findings demonstrate that awareness regarding data localization does not differ across age

categories. Therefore, **Hypothesis 3 is not supported for this dimension**, as awareness varies significantly across age categories.

Q9. Do you believe personal data transferred outside India is adequately protected?

To examine whether perceptions of cross-border data security vary across age groups, “*Do you believe personal data transferred outside India is adequately protected?*” was analyzed using descriptive statistics and the Chi-Square Test of Independence. This item reflects the National Data Governance Awareness dimensions, which assess how citizens perceive the risk and protections associated with international data flow under the DPDP Act. Descriptive analysis (Table 6.30) highlights overall levels of confidence and concern among respondents, while the Chi-Square test (Table 6.32) determines whether these perceptions differ significantly across age categories.

Table 6.30: Perception about Cross-Border Data Transfer

Item	Responses	Frequency	Percentage
<i>Do you believe personal data transferred outside India is adequately protected?</i>	Maybe	170	42.5 %
	No	192	48. %
	Yes	38	9.5 %
	Total	400	100. %

The descriptive data show that respondents express substantive doubt regarding the safety of personal data transferred outside India. Nearly half of the respondents 48% believe such data is not adequately protected, while 42.5% opt for “*maybe*”, indicating uncertain or limited awareness of international data security mechanisms. Only 9.5% expressed confidence that the data transferred is adequately protected. This distribution suggests low public trust in cross-border data transfer safeguards.

Table 6.31: Perception about Cross-Border Data Transfer across Age Groups

Responses	18-25	26-35	36-45	46-60	Total
Maybe	142	15	12	1	170
No	135	42	12	3	192
Yes	33	2	3	0	38
Total	310	59	27	4	400

The data shows a strong lack of confidence among respondents regarding the protection of personal data transferred outside India. Across all age groups, “no” and “maybe” responses dominate, with 192 (48%) respondents saying no and 170 respondents (42.5%) saying maybe. Only 38 respondents (9.5%) across the age group believe such data is adequately protected.

Table 6.32: Chi-Square Test Result (Perception of Cross-Border Data Transfer)

Test	χ^2 value	df	p-value
Pearson Chi-Square	16.925	6	.010
Likelihood Ratio	17.861	6	.007

Interpretation:

The Chi-Square test shows a Pearson χ^2 value of 16.925 (df = 6, p = .010) and a Likelihood Ratio of 17.861 (p = .007). Because both p-values are below 0.05, the relationship between age group and the belief that personal data transferred outside India is adequately protected is statistically significant.

Result:

The Chi-Square results (p < 0.05), perceptions of **cross-border data security differ meaningfully across age groups**. Younger respondents exhibit higher uncertainty, while older respondents show stronger skepticism. Hypothesis 3 is not supported for this dimension as awareness regarding international data transfer protection varies significantly across age categories.

Analysis of Hypothesis 3:

The analysis of hypothesis 3, which proposes that awareness of the Digital Personal Data Protection Act 2023 does not differ significantly across age groups in Nagaland, reveals a mixed pattern when examined across various awareness dimensions. This hypothesis predicts no significant difference in awareness between age groups. Therefore, if $p > 0.05$, the hypothesis is validated, and if $p < 0.05$, the hypothesis is not supported by the data. The value of p in the five awareness dimensions, consisting of nine questions, is discussed as below:

1. Basic Awareness (Q1) the Pearson Chi-Square $p = 0.042 (< 0.05)$ shows significant difference across age group. Therefore, the *hypothesis is not supported for Q1*.

2. Nagaland Context Awareness: Q2- Modification of laws for Nagaland, the Pearson Chi-Square $p = 0.186 (> 0.05)$ does not show a significant difference across age groups. Therefore, *the hypothesis is validated for Q2*. For (Q3) Nagaland-Specific Policies – Kruskal-Wallis $p = .484 (> 0.05)$ indicates that awareness does not vary significantly across age categories. The awareness in this dimension appears uniform across generations. Therefore, *the hypothesis is validated for Q3*.

3. Digital Readiness Awareness: Q4- Confidence in India's cybersecurity infrastructure- the Pearson $p = .106 (> 0.05)$ shows no significant difference among age groups, *supporting the hypothesis*. For Q5- Effect of internet access and digital literacy- the Pearson $p = 0.036 (< 0.05)$ shows a significant relation between age and awareness of the role of internet access and digital literacy in the implementation of data protection laws. Therefore, the *hypothesis is not supported by the data*. And for Q6- Need for digital infrastructure investment- the Pearson $p = .324 (> 0.05)$ non-significant p -value of 0.324 shows broad agreement across all age groups and *validates the hypothesis* for this question.

4. Personal Data Protection Awareness (Q7) the Pearson $p = 0.700 (> 0.05)$. The value shows no statistically significant difference across the age groups in their confidence regarding online data protection. Therefore, *Q7 supports the hypothesis*.

5. Data Governance Awareness: Q8. Data localization improves security- the Pearson $p = 0.02$ (< 0.05) indicates that age groups differ in their understanding of the security implications of storing data within India. Therefore, the ***hypothesis is not supported by data***. For Q9. Cross-Border data adequately protected- the Pearson $p = 0.01$ (< 0.05) p-value shows that perceptions of the protection of personal data transferred outside India vary considerably across age groups. Therefore, the ***hypothesis is not supported by data***.

Out of 9 questions, the hypothesis was validated ($p > 0.05$) for Q2, Q3, Q4, Q6, and Q7 and rejected ($p < 0.05$) for Q1, Q5, Q8 and Q9. This means the age groups differ significantly in 4 key areas of awareness, especially basic awareness (Q1), digital literacy (Q5), data localization (Q8) and cross-border data transfer (Q9), the core component of overall awareness. Therefore, the hypothesis 3 “*Awareness of the Digital Personal Data Protection Act 2023, among the citizens in Nagaland, does not differ significantly across age groups*” cannot be fully validated. Instead, the cumulative evidence shows that awareness of the DPDP Act varies across age groups in several important aspects. As a result, **the hypothesis is partially validated**.

6.5 ANSWERS TO RESEARCH QUESTIONS

The study is guided by the following key research questions:

RQ.1 What are the core features, guiding principles, and legal principles underlying the Digital Personal Data Protection Act 2023, and how do they compare with global data protection standards?

The Digital Personal Data Protection Act 2023 presents India’s first comprehensive legislative framework for safeguarding personal data in the digital domain. The Act embodies the principles of data autonomy, ensuring that individuals retain control over their personal data. At its core, the DPDP Act is guided by key principles such as consent-based data processing, purpose limitation, data minimization, storage limitation and accountability of data fiduciaries. It mandates that personal data be collected only for lawful purposes with explicit consent, and processed in a manner

that is fair, transparent and proportionate. Beyond access and correction, the DPDP Act recognizes the right of individuals to appoint a representative to exercise their rights is a novel feature not explicitly found in most global frameworks. The Act also establishes the Data Protection Board of India to oversee compliance, handle grievances, and impose penalties for violations. Special emphasis is given on the protection of children's data, the requirement for data fiduciaries to adopt security measures and the rights of individuals to access, correct, or erase their data.

When compared to global data protection frameworks, particularly the European Union's General Data Protection Regulation (GDPR), the DPDP Act reflects both alignment and divergence. It aligns with global standards in recognizing consent, transparency, and accountability as foundational principles. However, it departs from the GDPR in its broad scope for government exemptions and the centralization of regulatory authority under the Central Government, which may limit the independence of oversight mechanisms. Furthermore, the DPDP Act adopts a principle-based approach rather than the GDPR's right-based framework, focusing more on compliance obligations for organizations than on individual enforcement mechanisms. While the GDPR enshrines stronger safeguards such as the "*right to data portability*" and "*right to object to automated decision-making*", the DPDP Act introduces a more flexible, context-specific model to suit India's developing digital ecosystem. Another significant aspect is the Cross-Border Data Transfer under the DPDP Act, unlike the EU GDPR, which allows data to be transferred only to countries that meet strict adequacy standards, the DPDP Act adopts a more flexible model. It empowers the Central Government to notify countries where data transfer may be restricted. This flexibility also introduces certain ambiguity. This raises concerns about whether data protection levels in recipient countries will match India's data protection standards. Additionally, without clearly defined criteria or reciprocal agreements, there is a potential risk that personal data may be transferred to jurisdictions with weaker privacy safeguards, exposing individuals to misuse or inadequate redressal mechanisms.

Lastly, in terms of data localization, and data breach intimations, the DPDP Act departs from the earlier drafts that mandated strict local storage of sensitive

personal data. Instead, it introduces a flexible mechanism where the Central Government may notify specific countries or territories for cross-border data transfer. The Act does not explicitly address artificial intelligence, automated decision-making, and algorithmic accountability issues that are central framework in the EU GDPR and AI Act. On data breach intimation, the Act requires the data fiduciary to inform the Data Protection Board of India and affected individuals, in such manner as may be prescribed. However, it lacked detailed procedural guidance, timelines or a threshold for notification, unlike the GDPR's 72-hour rule. In essence, the DPDP Act 2023 marks a significant milestone in India's digital governance landscape, showing a shift from fragmented data regulations to a unified and structured approach. The Act lays a foundational legal architecture that aligns India with evolving international data protection norms.

RQ.2 What is the level of awareness and understanding among citizens in Nagaland regarding digital privacy rights, data protection mechanisms, and their responsibilities as data principals?

The DPDPA 2023 emphasizes the principles of informed consent and data subject empowerment; however, these principles can be meaningfully realized when citizens possess a clear understanding of their rights. The answer to the question is examined in three parts based on the empirical data collected, focusing on citizens' awareness of digital privacy rights, their understanding of data protection mechanisms and their perception of personal responsibilities as data principals.

1. Level of Awareness and Understanding among Citizens regarding Digital Privacy Rights:

The finding reveals that the citizens of Nagaland exhibit a moderate yet uneven level of awareness regarding digital privacy rights. As the data shows, the majority of respondents 66% were somewhat familiar with the concept of data protection, while only 18% considered themselves very familiar. These patterns reflect that, although the idea of digital privacy has gained general recognition, a deep understanding of the rights and implications remains limited. Awareness of privacy as a fundamental right

under the Indian Constitution was notably high, with 89% but only 30% respondents were aware of the right to be forgotten. This disparity illustrates a conceptual awareness practice gap in citizens who are conscious of privacy as a broad principle but lack clarity about their enforceable digital rights. Similarly, familiarity with the DPDP Act was low. This indicates that legal literacy on the data privacy framework has not yet penetrated the general population, despite growing digital participation. The near absence of public campaign underscores the deficiency of state-level engagement. The data reveals emerging awareness, but their comprehension of digital privacy rights remains largely fragmented and policy-disconnected. Many respondents recognize the term but lack in-depth comprehension of its legal, ethical and procedural dimensions.

2. Awareness and understanding of Data Protection Mechanisms:

The understanding of institutional and individual mechanisms for data protection is comparatively low and marked by skepticism. Most respondents expressed the belief that their data is not adequately protected when using online services, and further doubted that personal data transferred outside India is sufficiently secure. 97.5% reported that they have never received any information about how the organizations are using personal data. This shows near near-total absence of transparency and accountability for the organizations handling data. The majority of respondents agree that emerging technologies pose a risk to personal data; only 32 respondents disagreed. This indicates that although individuals might not be legally literate in data protection, they possess an intuitive sense of digital vulnerability. For sectoral prioritization patterns reveal where citizens perceive vulnerabilities, where 61% identified the banking sector as most in need of enhanced protection, followed by healthcare and government services.

3. Understanding of Responsibilities as Data Principals:

When it comes to individual responsibilities, the findings reveal a low level of proactive engagement with personal data security practices. While citizens express concern about digital risks, their behaviour often does not align with privacy practices

by individuals. The behavioural patterns suggest that citizens view data protection primarily as an institutional obligation, rather than a shared responsibility. The lack of routine privacy management actions, such as reviewing data-sharing policies or maintaining strong authentication, reflects a limited understanding of one's role as a data principal. Almost 77% (Agree + Strongly Agree) supported the idea that Nagaland should develop its own complementary data protection policy. This suggests strong public endorsement for a localized policy framework to address region-specific digital governance challenges. Moreover, 71% advocated for state investment in digital infrastructure, indicating a collective recognition that digital rights cannot be actualized without robust technological foundations.

The findings indicate that:

- General awareness of digital privacy rights is moderate to high (right to privacy), but specific legal and procedural awareness is low (DPDP Act and Right to be Forgotten).
- Citizens perceive risks associated with digital technology, yet lack behavioural discipline in practicing data protection.
- There exists a trust deficit towards organizations and skepticism about data security mechanisms.
- Support for stronger state-level regulation and infrastructure development reflects an emerging policy consciousness within the populace.

Thus, the level of awareness and understanding among citizens in Nagaland regarding digital privacy rights and data protection mechanisms is developing but insufficiently mature. The findings emphasize the need for targeted digital literacy initiatives, localized public outreach and culturally adapted awareness programs to transform citizens from passive digital users into informed, empowered, and privacy-conscious participants in the digital ecosystem.

RQ.3 Does the existing digital infrastructure in Nagaland support the practical enforcement of the Digital Personal Data Protection Act 2023?

Digital Infrastructure is fundamental to understanding the real-world applicability and effectiveness of the Digital Personal Data Protection Act 2023 within the context of Nagaland. The capacity of the State to implement and enforce data protection norms depends not merely on legal or institutional readiness, but also on the technological backbones that enable secure data generation, transmission, storage, and monitoring. In essence, digital infrastructure forms the enabling environment through which the principles of privacy, consent, and accountability can be practically realized. According to the State of India's Digital Economy Report 2024⁵⁵⁴, published by the Indian Council for Research on International Economic Relations (ICIER), Nagaland remains one of the Indian states in the nascent stage of digital ecosystem development. The report highlights significant disparities in digital penetration, broadband access, and institutional connectivity between Nagaland and more technologically advanced States. While India overall has made rapid progress in expanding digital public infrastructure but Nagaland's participation in this digital transformation remains partial and uneven.

The ICRIER report categorizes Indian states under the Digital Development Level (DDL) based on parameters such as digital infrastructure, digital payment, e-governance services, and digital literacy. Nagaland ranks in the lower quartile of this index, reflecting its limited capacity to fully integrate digital governance mechanisms. Internet connectivity remains constrained, particularly in rural and hilly areas, where network coverage is intermittent and broadband speeds are below the national average. These infrastructural bottlenecks directly affect the ability of state departments and comply with real-time reporting and monitoring obligations under the DPDPA. Thus, the current digital infrastructure in Nagaland does not yet fully support the practical enforcement of the DPDP Act 2023. The limitations are both technical and institutional. However, the state stands at a promising juncture with rising digital participation, public endorsement of infrastructural investment, and

⁵⁵⁴ Dr Deepak Mishra et.al, *State of India's Digital Economy Report 2024*, Indian Council for Research on International Economic Relations (ICRIER) 2024.

growing policy consciousness state possesses the foundational potential to strengthen its digital ecosystem.

RQ.4 To what extent do legal, policy and institutional reforms need to be introduced to ensure the effective enforcement of the Digital Personal Data Protection Act 2023, within the socio-legal context of the State of Nagaland?

The effective enforcement of the Digital Personal Data Protection Act 2023 in Nagaland requires a comprehensive reform approach that considers the state's socio-legal realities, institutional readiness and digital maturity. While the Act provides a strong national framework for safeguarding citizens' data rights, its implementation in Nagaland demands contextual adaptation to address regional challenges such as digital literacy, infrastructure limitations and weak policy mechanisms. The following points outline the key areas where reforms are needed to make the Act functional and enforceable in the state.

1. Establishment of a State-level Data Protection Authority

A dedicated Nagaland Data Protection Authority (NDPA) should be established to localize enforcement of the DPDP Act. This institution would monitor compliance, investigate breaches, and coordinate awareness programs. Currently, enforcement mechanisms are centralized at the national level, which limits responsiveness to state-specific issues such as cyber fraud in rural areas or misuse of data.

2. Integration of Data Protection in the State Legislation

To ensure legal consistency, Nagaland should integrate the principles of the DPDP Act into its state law and administrative regulations. This includes aligning existing IT, e-governance, and digital service policies with the central framework. State rules can define a clear jurisdictional role for local institutions, enabling more practical enforcement across departments and agencies.

3. Development of a Comprehensive Digital Policy Framework

A Nagaland Digital Policy should be developed to include data privacy, data management and cybersecurity. The policy must emphasize ethical data use, citizens' consent, and transparency standards. Such a framework will provide the legal and operational basis for data handling for both private and public sectors.

4. Strengthening Institutional Capacity and Technical Infrastructure

The lack of robust digital infrastructure remains one of the biggest challenges to enforcement. Institutions must be equipped with a secure data server, encryption systems, and audit mechanisms. Capacity-building programs to train government officers and IT personnel on the procedural and ethical aspects of the DPDP Act, enabling consistent application of privacy principles at the operational level.

5. Introduction of Digital Literacy and Privacy Awareness Campaigns

Effective legal enforcement requires informed citizens. The state should launch digital literacy and data privacy campaigns at both rural and urban levels. These campaigns must be multilingual, accessible, and culturally contextual, ensuring that every citizen understands their rights as data principal and their responsibilities in the digital environment.

6. Establishment of Grievance Redressal Mechanisms

A decentralized grievance redressal system is essential to enable citizens to report data misuse or breaches efficiently. Local Data Protection Cell could be set up at the district level under the supervision of the National Data Protection Authority to ensure accessibility, especially for rural areas with limited digital exposure.

7. Inclusion of Socio-Legal and Cultural Sensitivities in Implementation

Reforms must consider the unique socio-cultural context of Nagaland, where community networks and traditional governance play an important role. To strengthen this approach, awareness of digital privacy rights and citizens' responsibilities as data

principals must be promoted in local languages through culturally relevant mediums such as village councils, churches, student bodies and local media.

Thus, the enforcement of the DPPD Act in Nagaland requires multiple layers of reforms that address not only legal and technical limitations but also cultural, educational, and institutional dimensions. Legal reforms must be supported by digital infrastructure investment, policy innovation, institutional strengthening, and mass awareness of data rights.

6.6 APPLICABILITY OF DATA PROTECTION LAWS IN THE STATE OF NAGALAND

The study adopts a five-dimensional analytical framework to examine the doctrinal, institutional and societal factors shaping the implementation of the Digital Personal Data Protection Act 2023⁵⁵⁵ in Nagaland. This section evaluate both the extent and the practical feasibility of implementation in the State of Nagaland.

1. Central Legislative Competency and Applicability of the DPDP Act 2023 in Nagaland

The central law coverage dimension examines the constitutional authority of parliament to enact and enforce the Digital Personal Data Protection Act 2023 across the territory of India, including Nagaland, which enjoys special constitutional status under Article 371(A).

(i) Constitutional Competency of Parliament

The Seventh Schedule of the Indian Constitution provides a structured division of legislative authority among the Union and States through three lists: List I (Union List), List II (State List), and List III (Concurrent List). Matters not expressly enumerated in the State or Concurrent list fall within the residuary domain of parliament under Article 248. Since the regulation of personal data and digital privacy was not contemplated during the framing of the Indian Constitution and does not

⁵⁵⁵ Digital Personal Data Protection Act 2023, (No. 22), Act of Parliament, 2023 (India).

explicitly appear in any lists, it must necessarily be viewed as a residuary subject. Furthermore, aspects of digital communication, data transmission, and cyber governance fall under Entry 31 of the Union List, which vests Parliament with authority over “*post and telegraph; telephone, wireless, broadcasting and other like forms of communication*”⁵⁵⁶. Hence, the subject of digital personal data protection falls within the exclusive legislative competence of Parliament. The DPDP Act 2023, being a central enactment under this, is therefore applicable throughout India, including the territory of Nagaland.

(ii) Territorial and Jurisdictional Scope

The applicability scope of the Act is delineated primarily through section 3 of the DPDP Act 2023. Section 3⁵⁵⁷ clarifies the scope by specifying that the legislation applies to processing personal data within India, where the data is collected either directly in digital form or in non-digital form and subsequently digitalized. It also extends extraterritorially to data processing activities conducted outside India when such processing is connected to the offering of goods or services to individuals within India. Collectively, these provisions ensure that the DPDP Act governs all entities, whether government or private, domestic or international, whose data processing activities have a nexus to India. This includes data collected or maintained by the state agencies, local authorities, and even traditional or community institutions that engage in any form of digital data handling. Moreover, the extraterritorial clause ensures that international digital platforms and service providers offering goods or services to residents of Nagaland are equally bound by the obligations and safeguards prescribed under the DPDP Act 2023.

⁵⁵⁶ INDIA CONST. art. 24, Entry 31.

⁵⁵⁷ Digital Personal Data Protection Act 2023, § 3, Subject to the provisions of this Act, it shall-
(a) apply to the processing of digital personal data within the territory of India where the personal data is collected- (i) in digital form; or (ii) in non-digital form and digitised subsequently;
(b) also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India.

2. State Autonomy under Article 371(A)

The question arises as to whether Nagaland's special constitutional status under Article 371(A) might limit the operation of the Act within its territory. Article 371(A) provides that no Act of Parliament shall apply to Nagaland in respect of religious or social practices of the Nagas, Naga customary law and procedure, administration of civil and criminal justice according to customary law, and ownership or transfer of land and its resources, unless the State Legislative Assembly so resolves. However, the DPDPA does not regulate any of these protected domains. It concerns digital data governance, privacy and technological regulation. Therefore, the operation of the DPDP Act in Nagaland does not infringe upon the constitutional guarantees enshrined in Article 371A⁵⁵⁸.

3. Local Governance

The third analytical dimension, local governance, explores data protection within the decentralized administrative and customary systems that underpin governance in Nagaland. This dimension explores how institutions such as the village council and the Dobashi Courts engage with the responsibilities and challenges associated with implementing data protection norms under the Digital Personal Data Protection Act, 2023. These bodies serve as the primary interface between the citizens and the state. However, the local governance landscape in Nagaland is distinct from that of most Indian states because of its societal organization, where data is often regarded as a communal resource rather than an individual possession. In traditional Naga society, information about individuals, such as family lineage, land ownership, is embedded within collective identities and shared within the community. This communitarian understanding of data ownership contrasts sharply with the individual-centric rights recognized under the DPDP Act, which treats personal data as a matter of individual autonomy and consent. Further, the existing grassroots governance bodies, including

⁵⁵⁸ INDIA CONST. art. 371(A) Special provisions with respect to the State of Nagaland.-(1) Notwithstanding anything in this Constitution,- (a) no Act of Parliament in respect of – (i) religious or social practices of the Nagas;(ii) Naga customary law and procedures;(iii) administration of civil and criminal justice involving decisions according to Naga customary law;(iv) ownership and transfer of land and its resources, shall apply to the State of Nagaland unless the Legislative Assembly of Nagaland by a resolution so decides.

the village council and the Dobashi Courts, are predominantly composed of elderly leaders who command deep respect and legitimacy in customary governance but often possess limited exposure to digital technology and data privacy concepts. The lack of familiarity with concepts such as data consent, data minimization, or data protection may hinder the effective applicability of data protection laws.

4. Existing State Data Protection Practice

The fourth dimension is the Existing Data protection practices, which explores the prevailing landscape of data collection, processing, storage, and sharing across both public and private sectors in Nagaland. It seeks to understand how the State's current administrative and technological practices correspond with the national framework. A significant recent development in this regard is the adoption of the *Nagaland State Data Sharing and Accessibility Policy 2024*⁵⁵⁹. This policy represents the State government's proactive step towards institutionalizing data governance by establishing structured norms for data sharing, access and utilization across departments. It aims to promote data-driven decision-making, improve interdepartmental coordination, and enhance transparency and accountability in governance. The policy further outlines the establishment of a Project Management Unit (PMU) and a Data Dissemination Cell in each department, responsible for maintaining compliance, standardizing metadata formats and overseeing access permissions. While these measures represent a commendable attempt to bridge the gap between state-level data administration and national legal standards, their practical implementation remains contingent on the State's digital readiness and institutional capacity.

5. Institutional Compliance Practices (Banking and Health Care Sector)

The sixth analytical dimension, institutional compliance, evaluates the extent to which public and private institutions in Nagaland are prepared to operationalized the provisions of the Digital Personal Data Protection Act 2023. This dimension focuses

⁵⁵⁹ Nagaland State Data Sharing and Accessibility Policy, 2024, *The Nagaland Gazette* (Part- IIA, Mar. 29, 2025).

on the institutional capacity to adopt and internalize data protection norms through robust governance frameworks, risk management mechanisms and accountability procedures. To examine the existing data protection practices in Nagaland, interviews were conducted with two banking professionals, medical professionals and a representative of a private hospital. The purpose of these interviews was to gain insight into the current mechanisms, procedures and institutional approaches adopted by these sectors, which are the largest data handling institutions in India. In the banking sector, institutions routinely collect Know Your Customer (KYC) data, including identity proof, address verification, and biometric identifiers, as part of regulatory obligations. Their approach to data governance exhibits a different way of approaching. One bank reported conducting regular training sessions on data privacy and compliance, while the other offered such training only occasionally, indicating inconsistent practices. Similarly, the adoption of artificial intelligence and machine learning tools for functions such as fraud detection and chatbot services was reported by one bank, whereas the other had not yet integrated such technologies.

In contrast, the healthcare sector presented a more complex picture, reflecting both progress and significant challenges. Hospitals routinely collect patients' medical records and consent forms, which contain highly sensitive personal and health information. Normally, these hospitals obtain written consent; however, there is no evidence of formal training programs on data privacy and the implications of digital data handling. Private hospital adheres to strict institutional policy for secure data handling and storage. The private hospital has a strict data retention policy, under which patients' records are preserved for only two years. Beyond this period, data is automatically removed from the archive, reflecting a limited data retention practice by the organisation. Only records that are routinely shared with external authorities are newborn children's records, which are uploaded to the government's U-WIN portal of the Ministry of Health & Family Welfare. This shows the asymmetry in institutional preparedness between sectors that are subject to national regulatory oversight. The absence of uniform privacy practices hinders the effective implementation of data protection laws in Nagaland. Thus, while the Digital Personal Data Protection Act 2023 is legally applicable as part of India's national legal framework, its practical

implementation in the state remains limited. The findings of this study reveal that structural and infrastructural challenges continue to hinder the full enforcement of the Act. The applicability of the DPPD Act 2023 in Nagaland depends not only on its legal validity but also on how deeply it is integrated into local governance, public awareness and institutional practices.

6.7 CHALLENGES IN EFFECTIVE IMPLEMENTATION OF DATA PROTECTION LAWS IN NAGALAND:

The framework for evaluating the applicability of data protection laws provides a comprehensive method for assessing their theoretical reach and practical adaptability. The true test of any legal regime lies in its capacity for effective implementation. In the context of Nagaland, this process is inherently complex due to the interplay between its socio-technological, infrastructural, and perceptual barriers that limit the effectiveness of data protection implementation. These challenges collectively shape the gap between legal formulation and functional enforcement, making it necessary to identify and address them through a contextual, inclusive approach. The following discussion outlines the key factors that act as barriers to the effective implementation of data protection laws in the State of Nagaland.

1. Limited Public Awareness and Legal Familiarity

One of the foremost challenges to the effective implementation of the DPDPA in Nagaland is the limited public awareness of data protection principles. The survey reveals a significant gap in public understanding of data privacy and digital rights. The majority of respondents were unfamiliar with the DPDPA. Awareness of nuanced rights such as the “Right to be forgotten” remains particularly low. While the public is broadly aware of the constitutional right to privacy, without adequate public sensitisation, the law's compliance becomes superficial and reactive rather than proactive and preventive.

2. Inadequate Digital Infrastructure

Effective enforcement of data protection depends fundamentally on robust digital infrastructure, an area where Nagaland continues to lag. Limited connectivity, uneven internet access and infrastructural bottlenecks in rural and hilly regions hinder real-time reporting, breach notification, and monitoring processes. The State of India's Digital Economy Report (ICRIER, 2024) ranks Nagaland in the lower quartile for digital development. These deficiencies not only restrict technological adoption by institutions but also impede citizens' access to secure digital platforms, posing a structural constraint on the operational success of data protection laws.

3. Lack of Institutional Capacity and Compliance Mechanisms

Institutional readiness to comply with DPDPA standards is still at a nascent stage in Nagaland. Both the public and private sector exhibits uneven practices regarding data governance. The absence of standard operating procedures limits organizational preparedness.

4. Absence of State-Level Regulatory Coordination

Although the DPPDA is central legislation, its implementation necessitates state-level administrative mechanisms to ensure localized enforcement in Nagaland, there is currently no dedicated authority or coordination unit to observe compliance, investigate breaches, or conduct awareness drives. The absence of such a body leads to fragmented institutional responses and limits the ability to adopt the central framework on Nagaland's governance ecosystem. The establishment of a "*State Data Protection Cell*" under the guidance of the Central Data Protection Board could bridge this institutional vacuum and ensure effective ground-level application. Currently, Nagaland lacks a centralized mechanism for reporting or monitoring data breaches. While most respondents supported the idea of establishing a localized reporting framework, they would ensure timely responses, accountability, and transparency.

5. Limited Policy Communication and Public Outreach

The near absence of awareness campaigns or institutional communication about data protection in Nagaland shows a critical policy gap. Despite the PDPDA's emphasis on informed consent, citizens remain uninformed about how their data is processed or stored. Even institutions seldom disclose their data usage practices. The lack of outreach erodes public trust and perpetuates uncertainty. Effective implementation will require strategic communication by both state and central agencies through multilingual awareness drives, workshops, and digital sensitisation programmes that connect legal concepts with the everyday experience of online privacy.

6. Limited Role of Local Governance Institutions

While village councils and traditional bodies are central to Nagaland's governance ecosystem, they currently have no formal role in digital governance or privacy enforcement. Their exclusion creates a disconnect between legal regulation and community-level implementation. Given the communal character of Naga society, any legal reform that overlooks these grassroots institutions risks facing resistance or apathy at the local level. A community-inclusive governance model where local bodies are sensitized and given advisory roles could significantly improve awareness, trust and compliance. The present institutional detachment remains a barrier to localized data protection enforcement.

7. Absence of Contextualized State Policies Complementing DPDP

While Nagaland has introduced the State Data Sharing and Accessibility Policy 2024, it primarily focuses on inter-departmental data exchange and open data governance rather than personal data protection. The lack of complementary state-level rules or guidelines aligning with DPDP provisions creates a policy vacuum. This disconnect between open data promotion and personal privacy safeguards may lead to conflict in objective transparency versus protection. A context-sensitive state policy framework that harmonizes both priorities is essential to operationalize the DPDP effectively within Nagaland's institutional and technological realities.

The challenges outlined above reveal that the issue of implementation is not merely administrative but deeply structural and contextual. It intersects infrastructural limitations and socio-cultural realities. Effective enforcement of data protection laws in Nagaland, therefore, requires a context-sensitive governance model that balances central legal standards with local administrative and cultural adaptations. These challenges highlight the interdependence of law and awareness that legislative intent alone cannot ensure compliance without societal understanding, institutional capacity and cultural resonance. For Nagaland, the applicability of data protection laws lies in integrating legal reforms with participatory governance, fostering cooperation between central and state institutions, and embedding data protection principles into public education and digital literacy initiatives.

6.8 CONCLUSION

The applicability and effectiveness of data protection laws in the State of Nagaland, with particular reference to the Digital Personal Data Protection Act 2023. Drawing from the empirical data provides a comprehensive understanding of how digital privacy and data protection are perceived and implemented within the socio-legal context of Nagaland. The analysis reveals that while citizens exhibit a growing awareness of digital privacy as a constitutional right, their understanding of specific legal provisions and mechanisms for data protection remains limited. The study found that only a small proportion of respondents were familiar with the Digital Personal Data Protection Act 2023 and rights such as the right to be forgotten. This shows that legal awareness has not been translated into practical literacy, indicating the need for widespread public awareness and sensitisation efforts. The study emphasizes the urgent need for legal, policy, and institutional reforms. These include establishing a state-level data protection authority, incorporating privacy principles into state policies and ensuring transparency among data-handling organizations. ***The study concludes that while the Digital Personal Data Protection Act 2023 is legally applicable to Nagaland, its practical enforcement remains partial and conditional.***

CHAPTER 7

FINDINGS, CONCLUSIONS, AND SUGGESTIONS

7.1 INTRODUCTION

The overall findings, conclusions and suggestions that have emerged from the study titled “*A Critical Legal Study on Data Protection Laws in India and its Applicability in the State of Nagaland*” are presented in the chapter. Having undertaken a detailed exploration of India’s evolving data protection framework from its constitutional foundations and statutory development to its administrative implementation and regional adaptability. The preceding chapters of this study have undertaken a comprehensive examination of India’s data protection framework, its legislative evolution, constitutional underpinnings, judicial interpretations, and comparative insights from global practices. Special attention has been given to understanding how these broader legal norms are translated into practice within the distinctive socio-political and administrative environment of Nagaland. This chapter aims to consolidate the insights gained through the preceding chapter, providing a coherent understanding of the research outcomes and their implications for policy development. The study has not only evaluated the adequacy of existing legal provisions but also explored their operational challenges in the State of Nagaland. In the context of increasing digitalization of governance and citizen interactions, the need for robust and context-sensitive data protection mechanisms has become central to the debate on privacy, human rights and digital justice. To present the outcome of the study, the chapter is divided into three major parts, each of which addresses a set of essential components that collectively represent the culmination of the study.

Part I- Summary of the chapters: Summary of chapters, offering a concise yet comprehensive recap of the conceptual discussions, legal analyses, theoretical underpinning and empirical observation presented in the preceding chapters.

Part II- Core Outcome of the Study and Conclusion: The Key findings, derived from the doctrinal and empirical analysis, highlight the strengths and weaknesses of India's evolving data protection regime. The last component of this part is the Conclusion, which synthesizes the broader implications of the findings.

Part III- Suggestions: Offers a forward-looking perspective grounded in the analytical and empirical observations of the study. These recommendations aim to strengthen India's data protection framework, promote inclusive and culturally relevant digital governance, and enhance administrative capacity and public awareness in the State of Nagaland.

7.2 SUMMARY OF THE CHAPTERS

Chapter 2: Genesis of Data Protection Laws in India - This chapter explores the evolution of data protection laws in India in different phases. This chapter provides an in-depth examination of foundational legal frameworks enacted between 2000 and 2022. This includes the landmark Information Technology Act 2000, which introduced statutory recognition of electronic records and cybersecurity norms. The rise of Aadhaar and the creation of a nationwide digital identity ecosystem further underscore the urgent need for comprehensive data protection mechanisms. Followed by the Supreme Court judgement in Justice Puttaswamy (2017), which recognized the right to privacy as a fundamental right and significantly shaped India's legal data privacy framework. This chapter assesses the contribution of expert committees of the Justice A. P. Shah Committee and the Justice B. N. Krishna Committee and provides a comparative overview of successive data protection Bills from 2019 to 2023. The chapter concludes with an examination of the Digital Personal Data Protection Act 2023 and its draft Rule 2025, and the Nagaland State Data Sharing and Accessibility Policy 2024, situating regional developments within India's broader data governance evolution.

Chapter 3: Conceptual Foundation and Multilayered Legal Frameworks for Data Protection in India- Chapter 3 provides a comprehensive conceptual and regulatory foundation for understanding data protection in India. It explores the nature and

typologies of data, key technological tools for data protection. Part II of the chapter examines India's multilayered legal framework and several sector-specific frameworks governing and codes of practices issued by regulatory bodies for data protection. Part III outlines the institutional architecture for data governance in India. Chapter 3 concludes by identifying critical gaps and challenges that shape India's dynamic data protection landscape.

Chapter 4: International Legal Frameworks on Data Privacy and Data Protection-

Chapter 4 provides a comprehensive overview of the international legal frameworks governing data privacy and data protection. The chapter begins by tracing the historical development of global data protection norms, from early soft-laws to binding international instruments. It highlights the foundational role of human rights documents such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights in shaping global privacy standards. This chapter analyze major international legal frameworks, including Convention 108+, OECD Guidelines, APEC Privacy Framework and various UN initiatives, emphasizing their contributions to universal data protection principles. Further, this chapter makes a detailed comparative study of regional leading data protection laws across the various regions and other landmark legislation that have shaped global best practices. The chapter concludes by underscoring the importance of international cooperation and coherent global norms to ensure the protection of privacy in an increasingly interconnected digital world.

Chapter 5: Critical Appraisal of the Digital Personal Data Protection Act 2023-

This chapter presents a comprehensive and critical appraisal of the DPPD Act 2023, and examines its constitutional foundations and practical implications within India's evolving data governance framework. It highlights key gaps in the Act's definitions, safeguards and obligations, aligning with institutional weakness in the enforcement architecture, particularly concerning the autonomy and capacity of the Data Protection Board. This chapter also evaluates challenges in cross-border data transfer rules, the wide scope of state exemptions, and the implications of algorithmic decision-making on citizen rights. The chapter concludes with reform-oriented recommendations

aimed at strengthening rights, enhancing institutional accountability and technology a technology-neutral data protection regime.

Chapter 6: Assessing the Applicability of Data Protection Laws in the State of Nagaland: An Analysis- This chapter evaluates the real-world applicability of India’s data protection laws within the socio-legal, administrative, and technological context of the State of Nagaland. The empirical foundation enables a nuanced understanding of how national data protection norms intersect with local realities. The study found that Nagaland, through digital governance initiatives, online service delivery, and e-commerce, has significantly increased data generation within the state. However, awareness of data protection rights remains low. The key concern identified is the limited institutional capacity within Nagaland to operationalize the mandates of the DPDP Act. The chapter concludes that while the DPDP Act 2023 is formally applicable to Nagaland, its effective implementation requires decentralized adaptation through local rules, community engagement, and awareness programs. This chapter underscores that data protection in Nagaland is not merely a question of legal application but of legal translation. Translating the values of privacy, consent and accountability into the socio-legal environment of Nagaland.

7.3 KEY FINDINGS OF THE STUDY

The key findings that emerged from the doctrinal and empirical analysis of the study, “*A Critical Legal Study on Data Protection Laws in India and its Applicability in the State of Nagaland*”, aim to assess India’s evolving data protection regime, particularly the Digital Personal Data Protection Act 2023 and evaluate its applicability within the socio-legal framework of Nagaland. Together, these findings offer a comprehensive understanding of how law, governance and regional adaptability intersect in shaping data protection in India. The findings are categorized into three dimensions:

- Lessons drawn from global best data practices.
- Identification of gaps and inconsistencies within India’s data protection framework, and
- Empirical insights derived from the regional context of Nagaland.

1. Global Best Practice in Data Protection-

The study's comparative analysis of global legal frameworks, such as the European Union GDPR and other Acts, reveals several best practices that can guide India's regulatory frameworks:

i. Right-based Approach: Global models emphasize the individual's inalienable right to data protection grounded in principles of dignity, autonomy and individual control over one's own data.

ii. Independent Regulatory Authority: Most of the advanced jurisdictions maintain autonomous data protection authorities with strong enforcement powers.

iii. Explicit Data Subject Rights: Frameworks such as the GDPR guarantee a comprehensive set of rights, including access, correction, portability and erasure, enabling individuals to exercise real control over their data.

iv. Strict Data Breach Protocols: Countries like the EU mandate that data breaches be reported within 72 hours, enhancing transparency and accountability.

v. Algorithmic Accountability: Regulating AI for automated decision-making and profiling ensures fairness and explainability.

vi. Cross-Border Data Governance: Global frameworks define clear adequacy standards for international data transfer, protecting citizens' data even beyond national borders.

vii. Privacy by design: International best practices integrate privacy safeguards at the system-designed stage, not merely as a legal compliance measure.

viii. Proportionate Penalties: The GDPR's tiered penalty structure encourages compliance while deterring negligence without overburdening smaller entities.

2. Gaps in the Existing Data Protection Laws-

An in-depth review of the Digital Personal Data Protection Act 2023 reveals the following gaps that require policy attention.

- i. Absence of a rights-based foundation:* Unlike the EU GDPR, the DPPD Act is more administrative in nature, focusing on compliance obligations rather than individual rights.
- ii. Limited Regulatory Autonomy:* The Data Protection Board of India operates under the central government, raising concerns over independence and impartiality.
- iii. Vague Cross-Border Data Transfer Rules:* The government's notification list system lacks clear criteria, leaving scope for arbitrary decisions.
- iv. Inadequate Provisions for AI Regulation:* The Act does not address algorithmic profiling, automated decision-making or AI ethics, which are crucial in the digital economy.
- v. Unclear Breach Notification Timelines:* The absence of strict reporting deadlines weakens accountability mechanisms.
- vi. Excessive State Exemptions:* Broad exemptions for government agencies dilute the principle of data privacy and limit oversight.
- vii. No Distinction for Sensitive Data:* Unlike earlier drafts, the DPDP Act removes the category of sensitive personal data, treating all data uniformly.
- viii. Weak Grievance Redressal Mechanisms:* The complaint process depends heavily on procedural rules yet to be framed.
- ix. Insufficient Emphasis on Data Localization:* The flexible approach promotes international business but compromises national data sovereignty.
- x. Limited Public Awareness measures:* The law does not provide explicit obligations for citizens' education or digital literacy, reducing its grassroots impact.

3. Empirical Findings- Regional Context of Nagaland

The survey reveals critical insights into public awareness, institutional readiness and socio-legal compatibility of the DPDP Act.

i. Low awareness levels: Only a small segment of respondents had heard of the DPPD Act or understood its relevance, reflecting limited public outreach.

ii. Generational divide in digital literacy: Younger respondents display higher familiarity with data protection concepts compared to older age groups.

iii. Limited Institutional Capacity: Many local officers and organizations lack formal data protection mechanisms or trained personnel to ensure compliance.

iv. Need for Context-Specific Legal Adaptation: The survey indicates 55% believe that for effective data protection in Nagaland, a hybrid governance model is required, one that aligns national legal standards with traditional systems for collective responsibility and community governance.

v. Public Concerns over Government Data Practices: 57.5% of the respondents show concern about the misuse of the data collected by the government agencies. This shows a significant level of public mistrust of how personal data is handled by the government. This highlights the need for greater accountability and citizen awareness initiatives.

vi. Key obstacles to implementation: the survey shows that the lack of awareness (59.3%) is a major factor in the effective implementation of the DP laws in Nagaland.

vii. Weak Infrastructure readiness: Poor internet connectivity and limited infrastructure constrain the practical implementation of data protection measures.

viii. Need for local adaptation: 90.3% of the respondents express support for a localized data protection framework that integrates the DPPD Act with the unique socio-legal context of Nagaland.

ix. Public trust deficit: Many respondents express less trust in how organizations are handling their data. This shows a lack of organizational transparency practices while collecting data.

x. Potential for hybrid governance: The coexistence of customary data management practices and national laws offers a model for culturally grounded and participatory data governance.

7.4 CONCLUSION

The concluding reflection of the study was derived from both the doctrinal and empirical analysis. The study has explored the dynamic relationship between national legal developments and regional socio-legal realities. The study concludes that India's Digital Personal Data Protection Act 2023 represents a significant milestone in the country's transition towards a comprehensive and unified framework for data governance. It reflects India's growing recognition of privacy as a fundamental right and acknowledges the necessity of regulating data in an increasingly digitalized society. The Act establishes essential principles of consent, accountability, data minimization, and purpose limitation, thereby laying the groundwork for safeguarding individual autonomy and data privacy. However, the findings reveal that while the Act is a step in the right direction, it remains administrative rather than right-based, lacking robust mechanisms to ensure citizens' control over their data. A comparative analysis with global best practices demonstrates that India's framework aligns with international principles of consent fairness and proportionality but diverges significantly in enforcement autonomy, state exemptions, and public accountability. The DPDPD Act centralized regulatory authority, raising concerns regarding institutional independence. Moreover, the absence of explicit provisions on algorithmic accountability, AI regulation and cross-border data adequacy highlights the need for a more comprehensive and technologically neutral approach.

The survey data offers vital insights into how national data protection frameworks interact with regional socio-legal realities. The result demonstrates that while the Digital Personal Data Protection Act 2023 is formally applicable to

Nagaland, its practical enforcement faces considerable challenges. Low awareness and limited institutional constraints remain major barriers to compliance. The findings further reveal a strong public demand for a localized or hybrid governance framework that harmonize the principles of national data protection with local governance. The study also emphasizes that community-centric governance and individual-centric data protection are not inherently contradictory; both can coexist through a dual-layered model, where individual privacy rights under the DPPD Act are protected within a broader community governance framework grounded in customary norms. The findings underscore the need for a contextual adaptation of the Digital Personal Data Protection Act 2023 in Nagaland through state-specific rules, decentralized administrative mechanisms, and community-led awareness programs. Furthermore, strengthening digital infrastructure, capacity building of local institutions, and legal literacy initiatives will be essential for meaningful implementation. The study thus advocates for a global approach integrating global principles, national frameworks and local realities to achieve a balanced, inclusive and culturally sensitive data protection regime. This study concludes that the future of data protection in India depends not merely on legislative enactment but on effective translation of legal principles into socio-cultural contexts. For a state like Nagaland, the goal should not be to replicate national models mechanically but to adapt them in a way that reflects local governance and shared responsibilities.

7.5 SUGGESTIONS AND RECOMMENDATIONS

Based on the findings and conclusions of this study, this section presents recommendations aimed at strengthening India's data protection regime and ensuring effective implementation in the state of Nagaland. These recommendations draw from global best practices, doctrinal analysis and empirical data collected during the study. These suggestions were organized into two levels: (1) national-level policy reforms and (2) state-specific recommendations for Nagaland for an adaptive model of data protection governance.

1. NATIONAL-LEVEL RECOMMENDATIONS

i. Reintroduce the concept of Sensitive Personal Data (SPD): legal frameworks should restore the distinction between personal and sensitive personal data. Data related to health, biometric, and financial status requires more safeguards, aligning with global best practices.

ii. Regulate Artificial Intelligence and Automated Decision-Making: given the exponential growth of AI-based data processing, the law should include specific provisions for algorithmic transparency, bias mitigation, and accountability. A dedicated regulatory mechanism on AI and Data Ethics could be established to oversee emerging technologies.

iii. Establish clear timelines for data breach notification: the government should prescribe strict timelines, such as the 72-hour rule for notifying individuals and authorities of data breaches.

iv. Enhance Public Awareness and Digital Literacy: Effective data protection depends not only on the law but also on awareness. The government should launch a sustained nationwide campaign, in regional languages, to educate citizens about their data rights, consent mechanisms and grievance redressal procedures.

v. Encourage Privacy by Design and Default: Organizations should be required to embed privacy safeguards in technological design, ensuring that systems, platforms and applications adhere to data minimization, security, and transparency principles from inception.

2. NAGALAND-SPECIFIC RECOMMENDATIONS

i. Develop a State-Level Data Protection Policy: The government of Nagaland should formulate a Nagaland Data Protection and privacy policy harmonized with the DPDP Act. This framework should define local implementation strategies, institutional roles and awareness measures.

ii. Establish State Data Protection Cell: A dedicated cell may be set up within the State's Department of IT and Communication to coordinate compliance, capacity building, and grievance redressal under the DPDPD Act.

iii. Integrate Customary Institutions in Governance: Village councils, tribal bodies and traditional institutions should be engaged as stakeholders in policy dissemination and awareness activities. This inclusion would enhance local legitimacy and align data governance with collective responsibilities.

iv. Promote Awareness through Local Governance organizations: Awareness campaign should be conducted at the grassroots level through local bodies, educational institutions and civil society organizations, emphasizing the relevance of digital privacy and data behaviour.

v. Capacity Building and Training: Training programs for government officials, IT Staff, and institutions handling data should be organized in collaboration with academic institutions. This will strengthen the state's administrative capacity for effective enforcement.

vi. Localized Legal Literacy Programs: Awareness initiatives in local languages, focusing on citizens' rights under the DPPD Act, can increase public participation.

vii. Regular State-Level Impact Assessments: Periodic reviews of the implementation status of the DPDPD Act in Nagaland should be conducted to identify challenges, track progress and recommend adjustments in alignment with evolving technological and social conditions.

The above recommendations emphasize that data protection must evolve as a multi-level, context-sensitive governance framework. At the national level, it requires a shift towards stronger rights protection, institutional independence and technological foresight. At the state level, local participation and legal adaptation are required for effective implementation. This approach would not only strengthen compliance but also enhance public trust in digital governance.

7.6 CONTRIBUTION TO THE SOCIETY

The study contributes to society by addressing one of the most pressing issues of the digital age: the protection of personal data and the safeguarding of individual privacy in an era of rapid technological transformation. The key contributions are as follows:

- (1) The study provides a replicable policy framework that other states with comparable digital and institutional limitations can adopt.
- (2) The study proposes a hybrid data governance model that integrates statutory compliance with community-based oversight, a policy that balances traditional governance structure with modern data protection requirements.
- (3) The study highlights the importance of developing state-level data protection cells, training programs, and awareness initiatives. That the digital policies do not remain urban-centric but are accessible to all citizens.

Concluding Observations

This study critically examines the evolving landscape of the data protection laws in India and evaluates their applicability within the distinct socio-legal context of Nagaland. The study sought to bridge the gap between law in theory and law in practice. The study explores that effective implementation requires more than legal compliance; it demands institutional readiness and public awareness, the need to harmonize national uniformity with regional diversity and individual rights with collective values. Law must evolve as a tool of empowerment, enabling individuals, communities and institutions to exercise their digital rights responsibly and ethically. As the digital landscape continues to evolve, the principles of privacy, autonomy and accountability must remain at the core of legal and policy frameworks. The journey towards effective data protection is not one of finality but an ongoing adaptation and refinement. This study reaffirms that the true test of India's data protection regime lies not merely in legislative enactment but in its capacity to resonate with the everyday realities of its people.

BIBLIOGRAPHY

BOOKS

ALESSANDRO MANTELERO, BEYOND DATA HUMAN RIGHTS, ETHICAL AND SOCIAL IMPACT ASSESSMENT IN AI, Information Technology and Law Series, Vol. 36, Asser Press.

ANGHRIJA CHAKRABARTY, ASHIMA OBHAN AND AMAR K SUNDRAM, DATA PROTECTION LAWS DEMYSTIFIED, OakBridge Publications, First Edition 2021.

APURV SARDESHMUKH, DATA PROTECTION LAW AND REGULATIONS, Thomson Reuters, First Edition 2019.

BUDDHADEB HALDER, PRIVACY IN INDIA IN THE AGE OF BIG DATA, Digital Empowerment Foundation (2017).

CARISSA VÉLIZ, PRIVACY IS POWER WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA, Transworld Publishers, 2020.

DARA HALLINAN, RONALD LEENES, SERGE GUTWIRTH AND PAUL DE HERT, DATA PROTECTION AND PRIVACY DATA PROTECTION AND DEMOCRACY, Vol 12, Oxford: Hart Publishing, 2020.

DR ANKITA YADAV, RIGHT TO PRIVACY AND DATA PROTECTION: SPECIAL REFERENCE TO INDIA, Satyam Law International, (2023).

DR. HARISH KUMAR VERMA ET. AL. PERSONAL DATA PROTECTION LAWS IN INDIA, Notion Press (Oct. 30, 2023).

D P MITTAL, COMMENTARY ON THE DIGITAL PERSONAL DATA PROTECTION ACT 2023, Commercial Law Publishers (India) Pvt Ltd, 2024th Edition (2024).

JUSTIN RYAN AND MARIO LAZO, AI DATA PRIVACY AND PROTECTION: THE COMPLETE GUIDE TO ETHICAL AI, DATA PRIVACY, AND SECURITY, Technics Publications (2024).

KIRAN DESHTA, RIGHT TO PRIVACY IN INDIA UNDER INDIAN LAW, Deep & Deep Publications (2011).

LUCIANO FLORIDI, THE ONLINE MANIFESTO BEING HUMAN IN A HYPERCONNECTED ERA, Springer Open, (2015).

MARY C LACITY AND LYNDY COON, HUMAN PRIVACY IN VIRTUAL AND PHYSICAL WORLDS: MULTIDISCIPLINARY PERSPECTIVES, Technology, Work and Globalization, (2024).

NAVI (VIJAYASHANKAR NA), GUARDIAN OF PRIVACY: A COMPREHENSIVE HANDBOOK ON DPDPA 2023 AND DGPSI: CERTIFIABLE AUDITS, MATURITY ASSESSMENTS, AND BIS STANDARDS FOR DATA PROTECTION PRACTITIONERS IN INDIA, Notion Press (2024).

PUNEET BHASIN, PRACTICAL GUIDE TO DIGITAL PERSONAL DATA PROTECTION ACT, 2023 LAW AND COMPLIANCE, OakBridge Publishing, First Edition (2024).

RAHUL MATTHAN, THE THIRD WAY INDIA'S REVOLUTIONARY APPROACH TO DATA GOVERNANCE, Juggernaut Books, (2023).

RK DUBEY AND AJAY VERMA, DATA PROTECTION AND PRIVACY IMPLEMENTATION: INDIA PERSPECTIVE, ISBN 9781712746356 (2019) Data Protection

Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth and Paul De Hert, Data Protection and Privacy: (In)visibilities and Infrastructures, Springer International Publishing, (2017).

UDAYAN MUKERJI, R K NAROOA, JURISPRUDENCE OF PRIVACY, OakBridge Publishing, First Edition (2024)

VIJENDER KUMAR ET. AL, PRIVACY AND DATA PROTECTION IN THE DIGITAL ERA, Satyam Law International, (2024).

ACTS/ BILLS AND RULES

Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.

Aadhar and Other Laws (Amendment) Act 2019.

Credit Information Companies (Regulation) Act 2005.

Digital Personal Data Protection Act 2023.

Digital Personal Data Protection Bill 2023 (Bill no 113 of 2023).

Digital Personal Data Protection Rules 2025.

Draft Digital Personal Data Protection Bill 2022.

Draft Health Data Management Policy 2022, April 2022, Version 02. National Health Authority.

Indian Evidence Act, 1872.

Information Technology Act, 2000.

Information Technology (Amendment) Act 2008.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rule 2011.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rule 2021.

Indian Telegraph Act, 1885.

Medical Termination of Pregnancy (Amendment) Act 2021.

Mental Healthcare Act 2017.

Nagaland State Data Sharing and Accessibility Policy 2024

Personal Data Protection Bill 2019, (Bill no 373 of 2019).

Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act 1994.

Right to Information Act 2005.

Rules for Administration of Justice and Police in Nagaland (Amendment) Act 1974 (Nagaland Act No 7 of 1974).

Rules for Administration of Justice and Police in Nagaland (Second Amendment) Act 1982, (Nagaland Act No 4 of 1983).

Rules for Administration of Justice and Police in Nagaland (Third Amendment) Act 1984 (Nagaland Act no 1 of 1987).

The Telecommunication Act 2023, (Act No 44 of 2023).

The Constitution of India 1950.

FOREIGN ACTS

Artificial Intelligence Act, Regulation (EU) 2024/ 1689 of the European Parliament and of the Council, (2024)

California Privacy Right Act 2020

California Consumer Privacy Act 2018, California Civil Code [1798.100- 1798.199.100]

Charter of Fundamental Rights of the European Union, 2000/C 364/01

Cybersecurity Law of the People's Republic of China 2017.

Data Protection Act 1970, Federal Republic of Germany.

Data Protection Act 1973 (SFS no.: 1973:289) Sweden.

Data Security Law of the People's Republic of China 2021 dated 10th June 2021.

European Union General Data Protection Regulation (GDPR) EU 2016/679, OJL 119

EU Artificial Intelligence Act 2024, Regulation (EU) 2024/1689 of the European Parliament.

French Data Protection Act 1978.

Personal Information Protection Act 2011, (No 10465), South Korea.

Personal Information Protection Act 2020, (Act no 16930) South Korea

Personal Information Protection (Amended) Act 2023, (Act no 19234) South Korea

Personal Information Protection Law 2021(PIPL) People's Republic of China (NPC) 2021

Personal Information Protection and Electronic Documents Act 2000, (SC 2000, c.5) Canada

Protection of Personal Information Act, 2013 (No. 4 of 2013), Republic of South Africa, 2013.

Privacy Act 1985 (R.S.C., c.P-21), amended on 6th March 2025 (Canada)

CASE LAWS

Anuradha Bhasin v Union of India & Ors (2020) 1 SCR 812.

California v Greenwood 486 US 335

Canara Bank v C S Shyam (2018) 11 SCC 426.

Data Protection Commissioner v Facebook Ireland Limited C-311/18 (2020).

Digital Right Ireland Ltd v Minister for Communications, Marine and Natural Resources, C-293/12 (2014).

Digital Right Ireland Ltd v Minister for Communications – C 293/12 and C-594-12 (2014).

Directorate of Revenue v. Mohd. Nisar Holia (2007) 12 SCR 906

District Registrar and Collector v. Canara Bank AIR 2005 SC 186

Dr. Sabu Mathew George v Union of India & Others – AIR 2018 SC 578

Florida v Riley 488 US 445

Gaskin v The United Kingdom (1989) 12 E.H.R.R. 36

Google Spain SL and Google Inc v Agencia, C-1 31/12

Govind v State of Madhya Pradesh- 1975 AIR 1378

Girish Ramchandra Deshpande v Central Information Commission (213) 1 SCC 212.

Griswold v Connecticut 381 U.S. 479, 482-487 (1965).

Joseph Shine v Union of India (2018) 11 SCR 765

Jorawar Singh Mundy @ Jorawar Singh Mundy v Union of India and Ors WP (C) 3918/2021 & CM Appl 19941/2021.

Justice K S Puttaswamy (Retd) and Anr v Union of India (2017) 10 SCC 1, AIR 2017 SC 4161.

Kaleidoscope (India)(P) Ltd. v. Phoolan Devi AIR 1995 Delhi 316

Karmanya Singh Saren v Union of India, SLP (Special Leave Petition (Civil) No. 804 of 2017).

Kharak Singh v. State of Uttar Pradesh- AIR 1963 SC 1295

Klass v Germany Application no. 5029/71 Judgment of September 6 1978

La Quadrature du Net C-470/21 (2024).

Malak Singh v. State of Punjab and Haryana 1981 SCR (2) 311

Malone v The United Kingdom Application no. 8691/79

Mangia v Union of India, WP (C) No 347 of 2017.

Manohar Lal Sharma v Union of India & Others- W.P (Crl) No 000314-2021

Maximillian Schrems v Data Protection Commissioner (CJEU, 6 October 2015)

M.P Sharma v. Satish Chandra (1954) 1 SCR 1077

Mr. X v. Hospital Z AIR 1999 SC 495

Ministerio Fiscal C-207/16 (2016).

M/S Intex Technology (India) Ltd v Ashok Kumar CS (OS) 487/ 2016.

Naveen Kumar R @ Naveen v State of Karnataka- Criminal Petition No 3173 of 2023.

Navtej Singh Johar & Ors. Vs. Union of India Thr. Secretary Ministry of Law and Justice- (2018) 7 SCR 379.

Nivedita Sharma v Bharathi Hexcom Ltd, Appeal no 52 of 2012.

Olmstead v United States 277 US 438

People's Union for Civil Liberties (PUCL) v. Union of India- AIR 1997 SC 568

Pooran Mal v Director of Inspection (Investigation) of Income-Tax, New Delhi- AIR 1974 SC 348

P.R. Metrani v. C.I.T 2007 (1) SCC 789

R K Jain v Union of India (2013) 14 SCC 794

R Rajagopal v. State of Tamil Nadu- AIR 1995 SC 264

Reklos and Davourlis v Greece 2009 ECHR 200

Roe v Wade 410 US 113

Rohit Shekhar v. Narayan Dutt Tiwari (2012) 12 SCC 554.

Rotary v Romania Application No. 28341/95, (Europe)

Rotaru v Romania Application no. 28341/95

R.M. Malkani v State of Maharashtra 1973 SCC (1) 471

Shreya Singhal v Union of India- AIR 2015 SC 1523

Smith v Maryland 442 US 735

Sredharan T v State of Kerala WP (C) No. 9478 of 2017

State v. Charulata Joshi (1999) 4 SCC 65

State of Maharashtra v. Madhukar Narayan Mardikar AIR 1991 SC 207

Subranshu Raot v State of Odisha WP (C) 4159/2020

Tele2 Sverige AB v Post-och telestyrelsen, C-203/15 (2026).

United States v Miller 425 US 435

Zulfiqar Ahmed Khan v Quintillion Business Media Pvt Ltd CS (OS) 642/2018

REPORTS/ POLICIES/ DIRECTIVES/DRAFTS

A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 2018.

AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation, European Data Protection Supervisor.

APEC Privacy Frameworks 2005, Asia-Pacific Economic Cooperation, December 2005.

APEC Privacy Frameworks 2015, Asia-Pacific Economic Cooperation, Published date August 2017.

APEC Cross-Border Privacy Rules System, Rules, Policies and Guidelines, November 2019.

A Unique Identity for the people Aadhaar: An Overview, Unique Identification Authority of India, Govt. of India.

Bank's Policy on Record and Data Retention (version 1.0), SBI Organisational Planning and Systems & Procedures Department, Corporate Centre, 2024.

Brickwork Rating, E-Commerce Market in India, Brickwork Research, October 2024.

Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs), Securities and Exchange Board of India, Aug 20, 2024.

David Mangan, The Relationship Between Defamation, Breach of Privacy and Other Legal Claims Involving Offensive Internet Content, Defamation Law in the Internet Age, Commissioned by the Law Commission of Ontario, July 2017.

Deepak Mishra, Mansi Kedia et.al, State of India's Digital Economy (SIDE) Report 20245, IPCIDE, ICRIER Indian Council for Research on International Economic Relations (ICRIER), Feb. 2024.

Dr Deepak Mishra et.al, State of India's Digital Economy Report 2024, Indian Council for Research on International Economic Relations (ICRIER) 2024.

Dr Michele Finck, Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data Protection law? European Parliamentary Research Service, European Union, July 2019.

European Health Data Space Regulations (EHDS), Public Health, European Commission.

Expert Committee Report on Amendments to IT Act 2000.

Handbook on European Data Protection Law, 2018 Edition, Council of Europe.

India's UPI: A Global front-runner in digital payment status, PIB Thiruvananthapuram, Oct 30, 2023.

Information Technology Action Plan 1998.

Information and Cyber Security Guidelines, Insurance Regulatory Development Authority of India, April 2023.

Macro and Fiscal Landscape of the State of Nagaland, NITI Aayog, Mar 2025.

Master Direction on Digital Payment Security Controls, Reserve Bank of India, RBI/2020-21/42, DoS.CO.CSITE.SEC NO. 1852/31.01.015/2020-21 dated February 18, 2021.

Measures for the Safe Application of Facial Recognition Technology, Cyberspace Administration of China, Ministry of Public Security of the People's Republic of China, March 13, 2025.

Meglana Kuneva, European Consumer Commissioner, March 2009.

Ministry of Electronics and Information Technology (MeitY) Government of India, Annual Report 2021-2022.

Ministry of Finance, Unified Payment Interface (UPI) provides an opportunity to other countries to learn from the Indian experience- Professor Carlo Montes, Cambridge Business School, Press Information Bureau, 27th February 2025.

National Ethical Guidelines for Biomedical and Health Research Involving Human Participants, Indian Council of Medical Research, (2017).

National Guidelines for AI Ethics, 23rd December 2020, Korea Information Society Development Institute.

NITI Aayog's National Strategy for Artificial Intelligence, AI for all, June 2018.

OECD Going Digital Toolkit Policy Note, The Impact of data portability on user empowerment, innovation, and competition, OECD, 2024.

OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data, OECD Legal Instrument, 1980.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, (2002).

OECD Guidelines for Multinational Enterprises on Responsible Business Conduct, OECD, 2023.

OECD Privacy Framework, OECD, 11th July 2013.

OECD, Review of Relevance of the OECD Recommendation on ICTS and the Environment, OECD Digital Economy Paper, Nov 2024 No. 370.

Office of the Privacy Commissioner of Canada, Guidelines for obtaining meaningful consent.

OPC, Principles for responsible, trustworthy and privacy-protective generative AI technologies, 7th December 2023.

Press Note, Ministry of Electronics and IT, January 04, 2018.

Prof Dr Phil et al, The Protection of Mental Privacy in the Area of Neuroscience, Societal, Legal and Ethical Challenges, EPRS, July 2024.

Professor Giovanni Sator (The impact of the General Data Protection Regulation (GDPR) on artificial intelligence), European Parliamentary Research Service, 2020.

RBI Circular on Storage of Payment System Data, RBI/2017-18/153, DPSS.CO.OD.NO. 2785/06.08.005/2017-2018, 2018.

Regulations on the Management of Algorithm Recommendations for Internet Information Services, Ministry of Industry and Information Technology, 2021.

Report by the Committee of Experts on Non-Personal Data Governance Framework, Ministry of Electronics and Information Technology, Government of India, 2020.

Reports by the Committee of Experts on Non-Personal Data Governance Framework.

Report of the Group of Experts on Privacy, Chaired by Justice A P Shah,, r 2012. Justice Ajit Prakash Shah Committee (2011).

Report of the Joint Committee on the Personal Data Protection Bill, 2019

Rising Northeast Investors Summit 2025.

Report Summary on A Free and Fair Digital Economy, PRS India.

Reserve Bank of India (Digital Lending) Directions 2025, RBI/2025-26/36. DOR.STR.REC.19/21.07.001/2025-, 2025

RBI Master Direction- Information Technology Framework for the NBFC Sector, Reserve Bank of India, RBI/DNBS/2016-17/53, Master Direction DNBS.PPD.No.04/66.15.001/2016-14 dated 8th June 2017

Salient Feature of the Digital Personal Data Protection Bill 2023, Ministry of Electronics and IT, 9th August 2023, PIB, New Delhi,

State of India's Digital Economy Report 2023, ICRIER Prosus, Centre for Internet and Digital Economy, Feb 2023.

Telecom Commercial Communications Customer Reference (Second Amendment) Regulations 2025, Telecom Regulatory Authority of India, 2025.

Telecom Regulatory Authority of India, Press Release No. 44/2025, Dated 29th May 2025.

Understanding EU Data Protection Policy, EU Policies Insights, European Parliamentary Research Service, January 2025,

Unique Identification Authority of India, Government of India, Aadhaar Saturation Report, Jun. 30, 2025.

Violina Barman, Connecting the North Eastern Himalayas: The State of Access, Digital Connectivity and Digital Inclusion in North Eastern Region of India, Council for Social and Digital Development (CSDD), 2023.

GAZETTE NOTIFICATIONS

Ministry of Electronics and Information Technology Notification, GSR 843 E, The Gazette of India, Pt. II, Sec 3(i), Nov. 13, 2025.

Ministry of Electronics and Information Technology Notification, GSR 846 E, The Gazette of India, Pt. II, Sec 3(i), Nov. 13, 2025

Government of Nagaland, No.ST/8-16/11/409, Nagaland Gazette Part IIA, March 29, 2025.

CONVENTION AND TREATIES

Asia-Pacific Economic Cooperation Privacy Framework 2005.

Convention 108+, Convention For The Protection of Individuals With Regard To The Processing of Personal Data, Council of Europe.

Charter of Fundamental Rights of The European Union 2000.

European Convention on Human Rights, Council of Europe.

International Covenant on Civil and Political Rights, 1966.

Universal Declaration of Human Rights 1948.

ARTICLES

Abhik Chaudhuri, *Internet of things data protection and privacy in the era of the General Data Protection Regulation*, Journal of Data Protection & Privacy, Volume 1, Number 1, Henry Stewart Publications (2016).

Abraham, Manu Mariyan & Dev, Shampa, *AI-driven surveillance in India: Reconciling privacy, national security and legal oversight*, Journal of Data Protection & Privacy, Henry Stewart Publications, vol. 8(2), pages 183-207, November 2025.

Advent of Privacy Era in India, *The Digital Personal Data Protection Rules, 2025*, Ernst And Young LLP.

Algorithm Charter for Aotearoa New Zealand, Algorithm Impact Assessment User Guide, New Zealand Government, Dec 2023.

Ana Mishova, Data Protection Laws Around the World: A Global Perspective, GDPR Local, August 16, 2024.

Anirudh Burman, *Will India's Proposed Data Protection Laws Protect Privacy and Promote Growth?*, Carnegie Endowments for International Peace, Mar. 2020.

Anirudh Burman and Upasana Sharma, *How Would Data Localization Benefit India?* Carnegie India, 2021.

Annie Badman and Mathew Kosinski, What is Data?, IBM, Oct. 01, 2024.

Anupriya, & Singh Chauhan, Krishna Deo, *Securing informational privacy in India's IoT governance: Looking through the lens of FASTag*, Journal of Data Protection & Privacy, Henry Stewart Publications, vol. 7(2), pages 125-151, February 2025.

Arne Hintz, Lina Dencik, et al., *Civic Participation in the Datafied Society: Towards Democratic Auditing?*, Data Justice Lab, July 2022.

A. Shobanadevi et. al. *Novel identity management system using smart blockchain technology*, Vol 13, International Journal of System Assurance Engineering and Management, 496-505 (2022).

Babu, R. Rajesh & Sista, Suren, *European data protection laws: Learnings and implications for Indian business*, Journal of Data Protection & Privacy, Henry Stewart Publications, vol. 1(2), pages 206-221, (2017).

Brückner, S., Dridi, A., Deshmukh, A. et al. *A user-driven consent platform for health data sharing in digital health applications*. *NPJ Digit. Med.* **8**, 699 (2025). <https://doi.org/10.1038/s41746-025-02147-3>

Bu-Pasha, S, *Cross-border issues under EU data protection law with regards to personal data protection*. *Information & Communications Technology Law*, 26(3), 213–228, (2017). . <https://doi.org/10.1080/13600834.2017.1330740>

Chacko, Mathew & Mishra, Shambhavi, 2023. *Benchmarking the Indian Digital Personal Data Protection Act 2023 against data protection frameworks in Singapore, the EU, US and Australia*, Journal of Data Protection & Privacy, Henry Stewart Publications, vol. 6(2), pages 110-119, December.

Charru Malhotra and Udbhav Malhotra, *Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India*, Vol. 70, Issue 3, Indian Journal of Public Administration, 516-531 (2024), Sage Publications.

David Reinsel, John Gantz and John Rydning, *The Digitalization of the World From Edge to Core*, IDC release a white paper with the support of Seagate, Nov 2028

Diya Sarkar Ghosh, et. al., *The Conundrum of Erasing Digital Footprints: A Regulatory Challenge*, Vol. 15, Jindal Global Law Review, 25-59 (2024).

Elena Abrusci and Richard Mackenzie-Gray Scott, *The Questionable Necessity of a New Human Right Against being Subject to Automated Decision-Making*, Vol 31, Issue 2, INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY, 2023.

George Barbara Crutchfield and Gaut Deorah Roach, *Offshore Outsourcing To India By U.S. And E.U. Companies Legal And Cross-Cultural Issues That Affect Data Privacy Regulation In Business Process Outsourcing*, BUSINESS LAW JOURNAL, 6 U.C Davis Bus. L.J 13 (2006).

Gupta, Indranath & Naithani, Paarth, 2023. *Right to be forgotten in case of search engines: Emerging trends in India as compared to the EU*, Journal of Data Protection & Privacy, Henry Stewart Publications, vol. 5(3), pages 297-309, (2023).

Indravesh and Dr. Surendra Kalyan , *A Review Study to analyze the international Data Protection Frameworks and Best Practices and analyse their applicability and relevance to the Indian Context*, Vol. 2, Issue 1, International Journal of Multidisciplinary Research in Arts, Science and Technology, 2024.

International Telecommunication Union, *Global Cybersecurity Index 2020 Measuring Commitment to Cybersecurity*, ITU Publications.

Jain, P., Gyanchandani, M. & Khare, N. *Big data privacy: a technological perspective and review*. J Big Data 3, 25 (2016). <https://doi.org/10.1186/s40537-016-0059-y>

Jane Bambauer, *Is Data Speech?*, Vol. 66: 57, Stanford Law Review, 2014.

Jennifer King and Caroline Meinhardt, *Rethinking Privacy in the AI Era*, Stanford University Human-Centered Artificial Intelligence, White Paper Feb. 2024.

Joan M Wrabetz, *What Is Inferred Data And Why Is It Important?*, American Bar Association, Business Law Section, 22nd August 2022.

Kishwar, Sanya Darakhshan & Sahani, Jaskaran Singh & Tyagi, Saumya, *Navigating India's Draft DPDP Rules 2025: Implementation challenges in protecting children's personal data*, Journal of Data Protection & Privacy, Henry Stewart Publications, vol. 8(2), pages 144-164, (2025).

Kolah, Ardi, *Will 'AI for All' become a reality for 1.4 billion citizens in India this year?*, Journal of Data Protection & Privacy, Henry Stewart Publications, vol. 6(3), pages 224-226, (2024).

Leyden, A. *Standards and the EU AI Act: legitimacy, state of play, and future challenges*. Information & Communications Technology Law, 1–31 (2025).

Marcin Szczepanski, *Is data the new oil? Competition issues in the digital economy*, European Parliamentary Research Service (EPRS), Jan 2020.

Mark J Taylor and Jeannie Marie Paterson, *Protecting Privacy in India: The Role of Consent and Fairness in Data Protection*, Vol. 16, Issue 1, Indian Journal of Law and Technology, (2020).

Md. Toriql Islam and Md. Ershadul Karim, *The Brief Historical Account of Global Data Privacy Regulations and the Lessons for Malaysia*, Sejarah: Journal of History Department, University of Malaysia, 2019.

Niklas Kossow, Svea Windwehr and Mathew Jenkins, *Algorithmic Transparency and Accountability*, Transparency International, Feb 2021.

Paul De Hert, et. al, *The right to data portability in the GDPR: Towards user-centric interoperability of digital services*, Vol. 34, Issue 2, Computer Law & Security Review, 193-203 (2018).

Paulo Camphanha Santana and Faiz Ayat Ansari, *Data Protection and Privacy as a Fundamental Right: A Comparative Study of Brazil and India*, Vol. 9, No. 3, Journal of Liberty and International Affairs, 2023.

Prof Dr. Phil et al, *The Protection of Mental Privacy in the Area of Neuroscience, Societal, Legal and Ethical Challenges*, European Parliamentary Research Service, July 2024.

Rina Arum Prastyanti and Ridhima Sharma, *Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India*, Vol. 4 No. 2, Journal of Human Rights, Culture and Legal System, (2024).

RK Singh and Vini Singh, *Beyond Consent: Ensuring Meaningful Protection of Genetic Data Under India's Digital Personal Data Protection Act, 2023*, Vol. 46, Issue 4, Journal of Indian Academy of Forensic Medicine, 562-567 (2024).

Robert Walters, *Cross-Border Data Flows: An Evolving Multi-Layered Regulatory Approach Required!*, Global Privacy Law Review, Volume 3, Issue 1 (2022) pp. 29 – 45. DOI <https://doi.org/10.54648/gplr2022004>

Samuel D Warren and Louis D Brandeis, *The Right to Privacy*, Vol. 4, No. 5, Harvard Law Review, 193-220, (1890).

Saroj Koul, et. al., *Stakeholders' Understanding of Data Privacy: Implications for Digital Credit Consumers*, Vol. 12, No. 1, Cogent Business & Management, 2025.

Sh Manoj Roy Sarkar, *The Evolving Landscape of Digital Privacy in India: Balancing Innovation and Data Protection by the Government*, Data Protection and Data Privacy by INTERNATIONAL CENTRE FOR INFORMATION SYSTEMS AND AUDIT, PursuIT, 9th Edition, e-Journal, 2024

Singh, Pushpit & Simon, Silvia Tomy, *Personal data monetisation model in India: Reimagining the contours of the Digital Personal Data Protection Act, 2023 through a market-oriented approach analysis*, Journal of Data Protection & Privacy, Henry Stewart Publications, vol. 7(3), pages 292-324, March (2025).

Soria-Comas, J., Domingo-Ferrer, J. *Big Data Privacy: Challenges to Privacy Principles and Models*. Data Sci. Eng. **1**, 21–28 (2016). <https://doi.org/10.1007/s41019-015-0001-x>

Steve Wood, *Global Cross-Border Privacy Rules and the new initiatives to support data free flow with trust*, A & O Shearman, July 19, 2023.

Sustainability Directory, *Statelessness in Digital Age and Human Rights?*, Sustainability Directory, Apr 15, 2025

The Development of the Data Protection: From the GDPR to Global Standards, Ailance 2B Advice, Jan 29, 2025

Vaid, Monisha, *Exploring the lives of youth in the BPO sector: Findings from a study in Gurgaon*, Health and Population Innovation Fellowship Programme Working Paper no. 10. (2009), Population Council.

Vasudha Khanna and Atul Kotwal, *Examining the significance of the Digital Personal Data Protection Act, 2023 in the Context of the Healthcare Industry: A Comprehensive Analysis*, Vol. 22, Discover Public Health, (2025).

NEWSPAPERS

Aroon Deep, “Digital Personal Data Protection Act Notified After Two Years, RTI Act Amended, The Hindu, (Updated November 14, 2025, 08:58 PM IST).

Ayan Pramanik, 850mn internet users key to India’s \$1 trillion digital economy: Report, The Economic Times, May 16th, 2018.

Carole Cadwalladr and Emma Graham Harrison, Revealed: 50 million Facebook Profiles harvested for Cambridge Analytica in major data breach, The Guardian, Mar 17, 2018.

Cybersecurity Firm Claims Data Leak of 750 Million Telecom Users, Dot Asks Telcos For Security Audit, Economic Times Telecom, Jan 30, 2024.

Dharmender Jhamb, Dark Patterns Pose a Growing Concern in India’s Digital Landscape, The Hindu, September 12, 2024

John Xavier, Explained What does the alleged CoWIN data leak reveal?, The Hindu, June 18, 2023.

Madison Minges, National Security and the TikTok Ban, American University, Jan 23, 2025.

M Imyu Longchar, Role of Dobashis in Naga Customary Law and Practice, Eastern Mirror, June 9, 2018.

Poulomi Saha, Air India data breach: Personal Info of 45 lakh people leaked due to sophisticated cyberattacks, India Today, May 22, 2021.

Rachna Khaira, Rs 500, 10 minutes, and you have access to billion Aadhaar details, The Tribune, January 04, 2018.

Sohn Ji-young, Korea to investigate Google's covert location data collection, The Korea Herald, Nov 23, 2017,16:05:48

Srivatsan KC, Domino's Pizza data breach: Company says financial information safe as data of 180 million users compromised, Hindustan Times, May 24, 2021.

ONLINE SOURCES

Alexandra Jonker and Alice Gomstyn, Structured vs. Unstructured data: What's the difference?, IBM, Feb 07, 2025.

Algorithmic Impact Assessment: User Guide, Ada Lovelace Institute, Feb 8th, 2022,.

Annie Badman and Mathew Kosinski, What is Metadata?, IBM, 21st Oct 2024

Digital Impact, The Characteristics of digitized information require us to think carefully about how we use it as a resource

Ian Funnell, Structured Data vs Unstructured Data vs Semi-Structured Data, Matillion Blog, May 09, 2025.

Himanshi Singh, "CoWIN Data Breach", Cyber Peace, Jun 17, 2023

Mitangi Parekh, "Cybersecurity Ventures Report on Cybercrime", Esentire, July 23, 2024

Stephanie Susnjara and Ian Smalley, What is blockchain?, IBM.

The Outsourcing History of India, Outsource2india

Tim Mucci and Cole Stryker, What is big data analytics?, IBM, 5th April 2024

Varuntorn, How Social Media Algorithms Shape Public Opinion, Media & Society, 8th April 2025

What are Smart Contracts on blockchain? IBM.

What is encryption? Google Cloud,

What is Data Protection and Privacy?, Clouidian

What is Homomorphic Encryption? IEEE Digital Privacy.

What is predictive analytics?, IBM, Aug 8, 2022

Zara Amir, How to Manipulate your Ad Algorithm, Evolve Dash Blog, 31st Dec 2024.

WEBSITES

<https://www.census2011.co.in/census/state/nagaland.html>.

<http://www.maphill.com/india/nagaland/location-maps/satellite-map/highlighted-country/>.

<https://www.mapsofindia.com/maps/nagaland/>.

<https://www.merriam-webster.com/dictionary/data>.

<https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.

<https://www.ibef.org/industry/ecommerce>.

<https://webtest.nagaland.gov.in/nla/about-us/>.

ANNEXURE -I

QUESTIONNAIRE AND INTERVIEW SCHEDULE

Section 1: DEMOGRAPHIC INFORMATION

1. Name: _____ (Optional)
2. What is your age group?
☐ 18-25 ☐ 26-35 ☐ 36-45 ☐ 46-60+
3. What is your gender?
☐ Male ☐ Female ☐ Prefer not to say
4. What is your highest level of education?
☐ High school ☐ Undergraduate degree ☐ Postgraduate degree
☐ Doctorate ☐ Other
5. Are you a resident of Nagaland?
☐ Yes ☐ No
6. What is your occupation?
☐ Student ☐ Government employee
☐ Private sector employee ☐ Business owner
☐ Self-employed ☐ Unemployed

Section 2: GENERAL AWARENESS ON DATA PROTECTION LAWS

1. How familiar are you with the term “data protection”?
(a) Very Familiar [] (b) Somewhat Familiar []
(c) Not Familiar []
2. Have you heard of the Digital Personal Data Protection Act 2023?
(a) Yes [] (b) No []
3. Have you ever read any documents or articles related to data protection laws in India?
(a) Yes [] (b) No []
4. Have you seen any public awareness campaigns related to data protection in Nagaland?
(a) Yes [] (b) No []

Section 3: AWARENESS ABOUT DATA PRIVACY AND RIGHTS

1. Are you aware of the “***Right to Privacy***” as a fundamental right recognized by the Indian Constitution?
(a) Yes ☐ (b) No ☐
2. Are you aware of the “***Right To Be Forgotten***” under data protection law?
(a) Yes ☐ (b) No ☐

Section 4: INDIVIDUAL EXPERIENCE ON DATA PRIVACY

1. Have you ever experienced a data breach involving your personal information?
(a) Yes ☐ (b) No ☐
2. Have you encountered any data protection issues that are specific to the state of Nagaland?
(a) Yes ☐ (b) No ☐

Section 5: PEOPLE'S PERCEPTION OF TECHNOLOGY AND DATA PROTECTION

1. Do you believe emerging technologies (AI, IoT) pose a greater risk to personal data privacy?
(a) Yes ☐ (b) No ☐ (c) Maybe ☐
2. Do u believe that technological advancements like encryption can mitigate data privacy risks?
(a) Strongly disagree ☐ (b) Disagree ☐ (c) Neutral ☐
(d) Agree ☐ (d) Strongly agree ☐
3. Should new technologies like AI and machine learning be regulated under data protection laws?
(a) Yes ☐ (b) No ☐

Section 6: PRIVACY PRACTICES BY INDIVIDUALS

1. How often do you change your passwords or take steps to protect your personal information online?
(a) Frequently ☐ (b) Occasionally ☐
(c) Rarely ☐ (d) Never ☐
2. How often do you check the privacy policies of websites or apps before using them?
(a) Always ☐ (b) Often ☐
(c) Sometimes ☐ (d)Rarely ☐
(e) Never ☐

Section 7: DATA PRIVACY AT THE WORKPLACE

1. How would you rate the effectiveness of data protection measures in your workplace on a scale of 1-5?
(a) 1 (Low) ☐ (b) 2 ☐
(c) 3 ☐ (d) 4 ☐
(e) 5 (High) ☐
2. In your opinion, which sector requires the most attention regarding data protection laws?
(a) Healthcare ☐ (b) Banking ☐
(c) E-commerce ☐ (d) Government ☐
(e) Other ☐

Section 8: DIGITAL GOVERNANCE AND PRIVACY COMPLIANCE

1. Have you encountered any organization providing you with information on how your data is used?
(a) Yes ☐ (b) No ☐
2. Do you think organizations in India are transparent about their data protection practices?
(a) Yes ☐ (b) No ☐ (c) Maybe ☐
3. Should companies be required to inform customers immediately in case of a data breach?
(a) Yes ☐ (b) No ☐
(c) Only in certain cases ☐

Section 9: IMPLEMENTATION OF DATA PROTECTION LAWS IN NAGALAND

1. Do you think Data Protection laws need to be modified to suit the specific needs of Nagaland?
(a) Yes ☐ (b) No ☐
2. Should Nagaland create its own data protection policies to complement national laws?
(a) Strongly disagree ☐ (b) Disagree ☐
(c) Neutral ☐ (d) Agree ☐
(e) Strongly agree ☐
3. Are you confident in the current cybersecurity infrastructure in India?
(a) Yes ☐ (b) No ☐ (c) Needs improvement ☐

4. Do you think internet access and digital literacy affect the implementation of data protection laws?
(a) Yes ☐ (b) No ☐
5. Should Nagaland invest in digital infrastructure to support data protection laws?
(a) Yes ☐ (b) No ☐ (c) Maybe ☐
6. What are the primary obstacles to implementing data protection laws in Nagaland?
(a) Lack of awareness ☐ (b) Limited resources ☐
(c) Cultural barriers ☐ (d) Lack of legal expertise ☐

Section 10: OPINION ON DATA LOCALIZATION

1. Do you think data localization will improve the security of Indian citizens' data?
(a) Yes ☐ (b) No ☐ (c) Maybe ☐
2. Do you believe your data is adequately protected when you use online services?
(a) Yes ☐ (b) No ☐
3. Do you believe personal data transferred outside India is adequately protected?
(a) Yes ☐ (b) No ☐ (c) Not sure ☐

Section 11: LEGAL REFORMS AND RECOMMENDATIONS

1. Do you believe the Digital Personal Data Protection Act 2023 adequately addresses data protection issues?
(a) Yes ☐ (b) No ☐ (c) Needs improvement ☐
2. Would you support a localized framework for data protection that respects both customary law and national regulations?
(a) Yes ☐ (b) No ☐

ANNEXURE -I

INTERVIEW SCHEDULE

1. Government Officials: District Commissioner

Objective: To understand the policy perspective and how data protection laws are enforced or adapted at the state level.

1. How does the state of Nagaland interpret and apply national data protection laws like the Digital Personal Data Protection Act 2023?
2. Are there any specific policies or state guidelines in place for protecting personal data in Nagaland?
3. How does the state's special legal status (under Article 371A) impact the implementation of national data protection laws?
4. Are there any specific challenges faced by the state in enforcing data protection laws, especially considering the state's unique digital infrastructure?
5. What kind of training and awareness programs are offered to government officials and public sector workers on data protection?

2. Customary Law Experts: Dobashi of the Customary Court

Objective: To assess the role of customary laws and practices in shaping data protection policies in Nagaland.

1. How do customary laws in Nagaland address the concept of privacy and the protection of personal information?
2. How are tribal communities informed about their rights to data protection and privacy in a digital environment?
3. In cases where customary law conflicts with central laws on data protection, how are disputes resolved?
4. Are there any existing customary regulations that deal with the collection, use, and sharing of personal data within the community?

3. Police Headquarters: Kohima

Objective: To understand the role of law enforcement in handling data protection violations and cybercrimes in Nagaland

1. How often do you deal with cases involving data breaches or cybercrime in Nagaland?
2. Are there specific laws in place that guide law enforcement in addressing data protection violations?
3. Are police personnel provided with training or capacity-building programs on data protection and privacy laws?
4. What kinds of complaints related to data privacy or misuse of personal information have been received in recent years?
5. Are there any local guidelines or protocols in place for law enforcement when dealing with digital crimes specific to Nagaland's context?

4. Data Protection Practice in Banks and Hospitals

Objective: To assess the data protection practices, privacy safeguards, and institutional accountability mechanisms in banks and hospitals.

1. What types of customer data are collected and stored by your bank?
2. What types of patient data are collected and stored by the hospital?
3. What training programs or awareness initiatives does your institution provide to staff regarding data privacy and legal compliance?
4. Does your institution use AI or machine learning tools (such as fraud detection systems or chatbots), and how do you ensure data privacy in their operation?
5. What mechanisms are in place in your institution to handle data breaches or privacy-related complaints?
6. How does your institution obtain and manage consent from individuals for collecting and processing their data?
7. What protocols or safeguards does your institution follow to ensure the secure handling and storage of data?

ANNEXURE -II

PARTICIPANT INFORMED CONSENT FORM

Research Title: *A Critical Legal Study on Data Protection Laws in India and Its Applicability in The State of Nagaland*

Name of Researcher: Ms. Sonia Nath

Name of Institution: Department of Law, Nagaland University, Lumami.

Consent Declaration:

Please read and check each box to confirm your consent:

- ☐ I have understood the information provided by the researcher.
- ☐ I understand that my participation is voluntary.
- ☐ I consent to data collection methods via Questionnaires.
- ☐ I understand that my data will be anonymised and treated with strict confidentiality.
- ☐ I consent for my data to be used in publications, presentations, or reports derived from this research.

By signing below, I confirm that I voluntarily agree to participate in this research study.

Participant's Full Name: _____

Signature: _____

Date: _____

ANNEXURE-III

Digital Personal Data Protection Act 2023

रजिस्ट्री सं० डी० एल—(एन)04/0007/2003—23 REGISTERED NO. DL—(N)04/0007/2003—23



सी.जी.-डी.एल.-अ.-12082023-248045
CG-DL-E-12082023-248045

असाधारण

EXTRAORDINARY

भाग II — खण्ड 1

PART II — Section 1

प्राधिकार से प्रकाशित

PUBLISHED BY AUTHORITY

सं० 25] नई दिल्ली, शुक्रवार, अगस्त 11, 2023/ श्रावण 20, 1945 (शक)
No. 25] NEW DELHI, FRIDAY, AUGUST 11, 2023/SRAVANA 20, 1945 (SAKA)

इस भाग में भिन्न पृष्ठ संख्या दी जाती है जिससे कि यह अलग संकलन के रूप में रखा जा सके।
Separate paging is given to this Part in order that it may be filed as a separate compilation.

MINISTRY OF LAW AND JUSTICE (Legislative Department)

New Delhi, the 11th August, 2023/Sravana 20, 1945 (Saka)

The following Act of Parliament received the assent of the President on the 11th August, 2023 and is hereby published for general information:—

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (No. 22 OF 2023)

[11th August, 2023.]

An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

BE it enacted by Parliament in the Seventy-fourth Year of the Republic of India as follows:—

CHAPTER I

PRELIMINARY

1. (1) This Act may be called the Digital Personal Data Protection Act, 2023.

Short title and
commencement.

(2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

Digital Personal Data Protection Rules 2025

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

NOTIFICATION

New Delhi, the 13th November, 2025

G.S.R. 846(E).— Whereas draft of the Digital Personal Data Protection Rules, 2025 were published, as required under sub-section (1) of section 40 of the of the Digital Personal Data Protection Act, 2023 (22 of 2023), *vide* notification of the Government of India in the Ministry of Electronics and Information Technology *vide* number G.S.R. 02 (E), dated the 3rd January, 2025, in the Gazette of India, Extraordinary, Part II, Section 3, Sub-section (i), dated the 3rd January, 2025, inviting objections and suggestions from all persons likely to be affected thereby, before the expiry of the period of forty-five days from the date on which copies of the Official Gazette containing the said notification were made available to public;

And whereas copies of the said Official Gazette were made available to the public on the 3rd January, 2025;

And whereas objections and suggestions were received from the public in respect of the said draft rules have been considered by the Central Government;

Now, therefore in exercise of powers conferred by sub-sections (1) and (2) of section 40 of the Digital Personal Data Protection Act, 2023 (22 of 2023), the Central Government hereby makes the following rules, namely: —

1. Short title and commencement. — (1) These rules may be called the Digital Personal Data Protection Rules, 2025.

(2) Rules 1, 2 and 17 to 21 shall come into force on the date of their publication in the Official Gazette.

(3) Rule 4 shall come into force one year after the date of publication of this Gazette.

(4) Rules 3, 5 to 16, 22 and 23 shall come into force eighteen months after the date of publication of this Gazette.

2. Definitions. — (1) In these rules, unless the context otherwise requires, —

(a) “Act” means the Digital Personal Data Protection Act, 2023 (22 of 2023);

(b) “techno-legal measures” means as referred to under rules 20 and 22;

(c) “user account” means the online account registered by the Data Principal with the Data Fiduciary, and includes any profiles, pages, handles, email address, mobile number and other similar presences by means of which such Data Principal is able to access the services of such Data Fiduciary; and

(d) “verifiable consent” means a consent as specified in rule 10 or 11.

(2) The words and expressions used in these rules and not defined, but defined in the Act, shall have the same meanings respectively assigned to them in the Act.

3. Notice given by Data Fiduciary to Data Principal. —The notice given by the Data Fiduciary to the Data Principal shall—

(a) be presented and be understandable independently of any other information that has been, is or may be made available by such Data Fiduciary;

(b) give, in clear and plain language, a fair account of the details necessary to enable the Data Principal to give specific and informed consent for the processing of her personal data, which shall include, at the minimum, —

(i) an itemised description of such personal data; and

(ii) the specified purpose or purposes of, and specific description of the goods or services to be provided or uses to be enabled by, such processing; and

(c) give, the particular communication link for accessing the website or app, or both, of such Data Fiduciary, and a description of other means, if any, using which such Data Principal may—

Nagaland State Data Sharing Policy 2024

March 29, 2025

The Nagaland Gazette, Part-IIA

515

NOTIFICATION**Dated Kohima, the 6th March, 2025.**

NO.ST/8-16/11/409 :: The Governor of Nagaland is pleased to notify the Nagaland State Data Sharing and Accessibility Policy, 2024 to provide an enabling platform for providing proactive and open access to data generated through public fund available with various Government of Nagaland Departments and institutions with immediate effect.

This has the approval of the Cabinet vide No. CAB-1/14/2023 dated 9th October, 2024.

Sd/-**K. LIBANTHUNG PATTON**

Deputy Secretary to the Govt. of Nagaland.

**GOVERNMENT OF NAGALAND
SCIENCE & TECHNOLOGY DEPARTMENT****Nagaland State Data Sharing and Accessibility Policy****1.0. PREAMBLE:**

The Government of Nagaland
embark upon establishment of
“Nagaland Spatial Data Infrastructure (NSDI)”,
in the line of National Spatial Data Infrastructure(NSDI)”
created vide SMP/25/003/05 Dated 13th June, 2006
of Department of Science & Technology, Government of India
recognising the potential utility of large quantity of data generated using public
funding through various government departments/organisations/institutes;
for planning and development.

The data sharing and accessibility shall be based on the principles of:
**Non Redundancy, Openness, Flexibility Standards, Interoperability, Quality,
Efficiency, Accountability, Intellectual Property Right (IPR) and Right to**

Information.

The Government of Nagaland hereby adopt
the “Nagaland State Data Sharing and Accessibility Policy (NSDP)”
to facilitate easy access and sharing of such Government owned data,
in open format for good governance.

ANNEXURE-VI

IEC Certificate



Institutional Ethics Committee (IEC)
Nagaland University
Lumami Campus, Zhuneboto – 798627



Ref. No: IEC/NU/2025/I-2.9

Date: 09.05.2025

CERTIFICATE

This is certified that Ph.D research work entitled “A Critical Legal Study on Data Protection Laws in India and its Applicability in the State of Nagaland.” is presented by **Ms. Sonia Nath** (Reg. No: PhD/LAW/00705) under supervision of **Dr. Rumi Dhar**, Department of Law, Nagaland University, in the Institutional Ethics Committee meeting held on 9th May 2025 at 11.00 AM.

The Institutional Ethics committee approved the research work. **The Approval Number is: IEC/NU/2024/II-2.9**, dated 09.05.2025.

Prof. Ranjit Kumar
Member Secretary
Institutional Ethics Committee
Nagaland University, Lumami

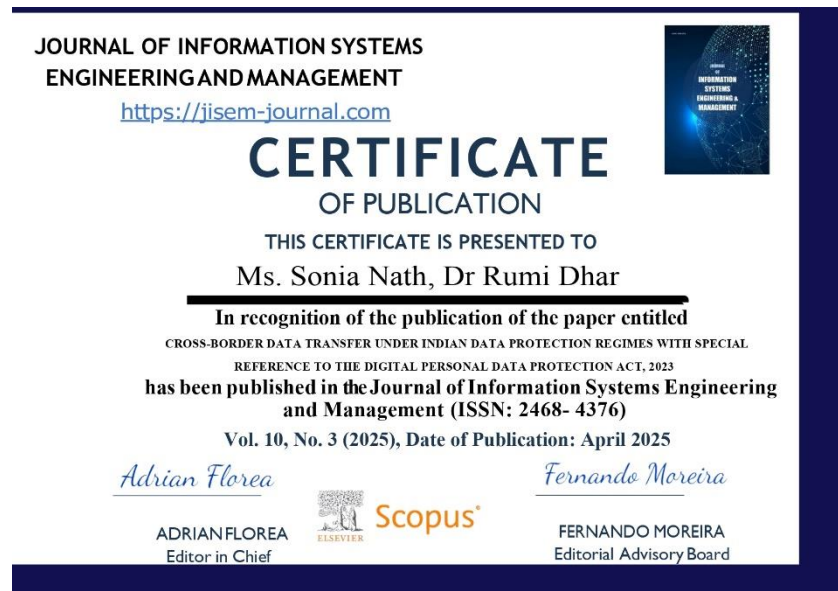
Prof. Bendang Ao
Chairman
Institutional Ethics Committee
Nagaland University, Lumami

ANNEXURE-VII

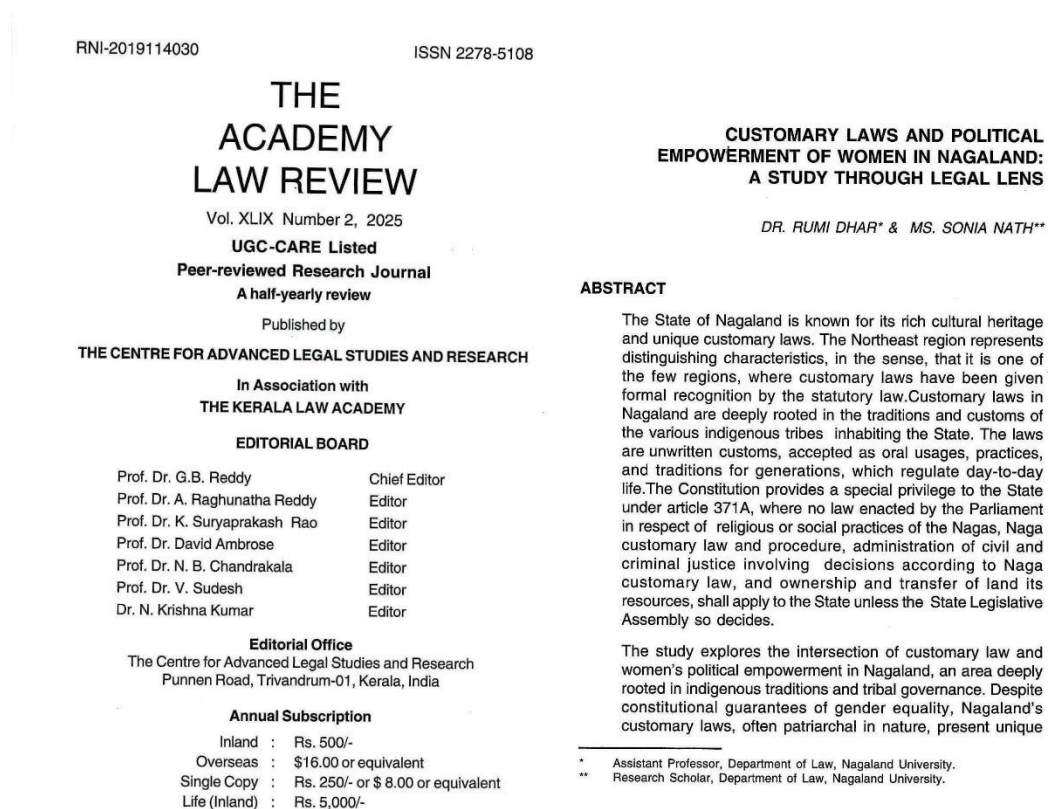
LIST OF PUBLICATIONS

Sl no	Name of Journal	Details of Journal	Title	Year Volume and Issue
1	Journal of Information Systems Engineering and Management	Scopus-Indexed Journal	Cross-Border Data Transfer Under Indian Data Protection Regimes With Special Reference To The Digital Personal Data Protection Act, 2023	Vol. 10 No. 3 (2025) Page 601-620
2	Academy Law Review	UGC Care-listed Journal	Customary Laws and Women's Political Empowerment in Nagaland: A Study Through Legal Lens	Vol XLIX, No 2 (2025) ISSN: 2278- 5108
3	The Chanakya Law Review Chanakya National Law University Patna	International Journal	Digital Surveillance And Civil Rights: Assessing The Impact On Privacy	Vol. V, Issue I Jan- June 2024 Pages 66-86
4	KDU Law Journal (General Sir John Kotelawala Defence University in Sri Lanka)	International Journal ISSN 2783-8870	Privacy Considerations In The Age of Digital Transformation In Emerging Bharat	Vol 4 Issue 2 (2024) Page 1-20

PUBLICATION 1: Journal of Information Systems Engineering and Management- Scopus-Indexed Journal



PUBLICATION 2: The Academy Law Review- UGC Care Listed



PUBLICATION 3: Chanakya Law Review (CLR) is an International Journal (E-Journal) Vol. V Issue I, Jan-June, 2024

CHANAKYA LAW REVIEW (CLR) Vol. V Issue I, Jan-June, 2024			
Sr. No.	Title of Paper	Author(s)	Page No.
1.	Women Prisoners And Their Rights: Special Need To Concern	Prof. Rajaram Garud & Dr. Anjali Boudar	2-18
2.	The Judicial System In Ancient India: Examination Regarding Hierarchy And Integrity	Mr. Amit Pandey & Dr. Swagat Pandey	19-27
3.	Legal Aid In India: Current Scenario And Future Challenges	Yasho Jain	28-35
4.	Cybernetic Conundrum: Decrypting Privacy Concerns Amid Governmental Data Regulation Efforts	Aanaya Gupta	36-55
5.	Democracy On Trial: In Reference To The Chandigarh Mayor Election Case	Muskan Suhag	56-65
6.	Digital Surveillance And Civil Rights: Assessing The Impact On Privacy	Dr. Rumi Dhar ¹ & Ms. Sonia Nath ²	66-86
7.	Dangerous Childhood: The Issue Of Child Soldiers With Special Reference To Armed Conflict	Shreyashi Raj & Ankit Kumar	87-102
8.	Evaluating & Re-Imagining Juvenile Justice: From Its Institution To Its Future	Palak Munaf Solkar & Ayush Mishra	103-118
9.	Green Tax: A Tool To Contain Corporate Environmental Crimes In India	Ms. Radha & Mr. Brjesh Kumar	119-133
10.	Is The Indian Political Opposition Structurally Weak? - Advocating For Opposition Rights	Alzaan Anwar & Devvrat Purohit	134-146



CHANAKYA LAW REVIEW (CLR)

VOL. V (ISSUE 01) JAN-JUNE 2024, pp. 66-86



DIGITAL SURVEILLANCE AND CIVIL RIGHTS: ASSESSING THE IMPACT ON PRIVACY

Dr. Rumi Dhar¹
Ms. Sonia Nath²

ABSTRACT

In an age characterized by swift technological progress and rapidly increasing security challenges, the surveillance landscape in India has experienced substantial transformation. The importance of safeguarding national security has led to the implementation of various surveillance laws; however, there is no specific legislation to govern surveillance in India, but the Information Technology Act of 2000 and the Indian Telegraph Act of 1885 are used to regulate surveillance. Laws pertaining to surveillance have been a subject of ongoing discussion, especially concerning the delicate balance between national security imperative and preserving the rights to privacy of individuals. The issue has become even more pressing in the digital age, where various government agencies and private companies collect and store enormous volumes of personal data. Addressing these concerns, India has recently passed the Digital Personal Data Protection Act 2023, which seeks to find an equilibrium between national security considerations and the safeguarding of individual privacy rights. Surveillance is a tool for maintaining the nation's sovereignty, unity, and integrity. Now, the question arises whether surveillance by the government violates the individual's right to privacy. The objective of the paper is to conduct a thorough analysis of the current laws and regulations pertaining to surveillance in India, evaluating their implications for the rights and liberties of individuals.

KEYWORDS: Right to Privacy, Digital Surveillance, Data Protection, and Digital Personal Data Protection Act 2023.

vii

¹ Assistant Professor, Department of Law, Nagaland University (a Central University) Nagaland, India, Email: rumidhar@nagalanduniversity.ac.in.
² Research Scholar, Department of Law, Nagaland University (a Central University) Nagaland, India, Email: sonia.n2022@nagalanduniversity.ac.in.

CLR (VOL. V ISSUE I) JAN-JUNE, 2024

Page | 63

PUBLICATION 4: KDU Law Journal, vol 4 Issue 2 (2024)



KDU Law Journal
General Sir John Kotelawala Defence University, Sri Lanka

Volume 04 Issue II
September, 2024
ISSN 2782 - 8870

Privacy Considerations in the Age of Digital Transformation in Emerging Bharat

Rumi Dhar^{*}
Sonia Nath^{**}

Abstract

In today's technologically advanced world, the concept of privacy has become more critical than ever before. With the digital transformation sweeping across the globe, individuals' privacy has come under intense scrutiny. This is especially true in emerging economies, where rapid technological advancements reshape the societal landscape. However, the digital revolution has also posed a significant challenge to individual privacy on digital platforms. The unauthorized access, collection, storage, and utilization of personal sensitive data have become a great concern. With the increasing reliance on digital platforms for communication, financial transactions, and other activities, individuals' risk having their sensitive information compromised. The enactment of the Digital Personal Data Protection Act 2023 aims to establish a comprehensive framework for processing and protecting personal sensitive data in India. The first section of the article discusses the various ways digital transformation has influenced privacy, and the second section discusses the existing legal provisions in India concerning data privacy. Finally, the article concludes with the need for robust data protection laws and regulations, as well as increased awareness and education on privacy rights and best practices for individuals and organizations. This paper aims to examine the aspects of data privacy in the context of digital transformation in emerging

^{*} Ph.D.(MKGVP/Varamu), LL.M. (Gauhati) LL.B. (Assam), Assistant Professor, Department of Law, Nagaland University, India.
^{**} LL.M. (Assam), B.A. LL.B. (Assam), Research Scholar, Department of Law, Nagaland University, India.

law.faculty@kdu.ac.lk

ANNEXURE-VIII

LIST OF PAPERS PRESENTED

Sl no	Organized By	Title	Presented at	Date	Mode
1	The Department of Sociology Nagaland University	Data Governance and Digital Infrastructure	National Seminar	27 th - 28 th February 2025	Offline
2	Department of Law, North-Eastern Hill University, Shillong, Meghalaya	Artificial Intelligence in The Dark Web: Exploring the Risk and Challenges in the Digital Era	National Seminar	18 th October 2024	Online
3	Kumar B.Ed College, Dhanbad, Jharkhand.	A Socio-Legal Study on the Use of Digital Technology in National Education Policy (NEP) 2020.	National Seminar	29 th -30 th May 2024	Online
4	Heritage Foundation, in collaboration with Dispur Law College, Guwahati.	Privacy Considerations in the Age of Digital Transformation in Emerging Bharat.	National Seminar	1 st – 2 nd March 2024	Offline
5	The Department of Economics, Nagaland University	The Digital Personal Data Protection Act 2023: Balancing Data Privacy and Growth in the Digital Economy.	International Conference	12 th -13 th October 2023	Offline
6	The Department of Business Administration Assam University, Silchar.	Data Privacy and Corporate Governance: A Study in the Light of Data Protection Laws in India.	International Seminar	14 th -16 th Septemb er 2023	Offline



CERTIFICATE OF PARTICIPATION



This is to certify that Ms. Sonia Nath, PhD Scholar, Dept. of Law
of Nagaland University
has presented a paper titled Data Governance & Digital Infrastructure
in the Two Day National Seminar on
Social Lives of Infrastructure in Northeast India: Navigating Diversity, Connectivity, and Resilience,
Sponsored by the Indian Council for Social Science Research (ICSSR), New Delhi & Nagaland University,
Organized by Department of Sociology, Nagaland University, Lumami on 27th and 28th February 2025.


(PROF. JAGADISH KUMAR PATNAIK)
Vice Chancellor
Nagaland University


(PROF. ATHUNGO OVUNG)
Head
Dept. of Sociology, NU


(DR. SANDEEP GUPTA)
Convenor
Dept. of Sociology, NU



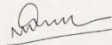
NCW Sponsored National Seminar on Harnessing AI Opportunities for Women

18th October, 2024

CERTIFICATE

This is to certify that ☒ Dr./Mr./Mrs./Ms.. Sonia Nath
Designation.. Research Scholar Institution Nagaland University has
participated/Chaired a session/Resource Person/Presented Paper ☒ in the NCW Sponsored National Seminar on
'**Harnessing AI Opportunities for Women**' held on **18 October, 2024** at Golden Jubilee Auditorium, North Eastern
Hill University, Shillong, Meghalaya.

The title of the paper was.. **AI in The Dark Web: Exploring the Risks and Challenges in the Digital Era**


Dr. Naveen Kumar
Co-Convenor, Organizing Committee
Department of Law,
NEHU, Shillong


Dr. A.K. Singh
Co-Convenor, Organizing Committee
Department of Law,
NEHU, Shillong


Prof. Jyoti J. Mozika
Coordinator & Head
Department of Law,
NEHU, Shillong

Multidisciplinary National Seminar On
“Emphasis of Technology in the National Education Policy-2020
(NEP-2020) for Transforming Education and Research”

Certificate

of Presentation
29th & 30th May, 2024



Organised by
Kumar B.Ed. College
Dhanbad, Jharkhand
(Affiliated to B.B.M.K.U., Dhanbad & JAC Ranchi, Jharkhand)
Recognized by:- ERC-NCTE NEW DELHI

Registration No. :- BBMKU/KBC-ICSRD-05-001-D1



In Association with
International Centre for Scientific Research and Development (ICSRD)
Bengaluru, Karnataka
(Indexed under MSME Act 2006 Govt. of India)
(ISO 9001:2015 Certified Organisation)

This is to certify that Prof. / Dr. / Mr. / Ms. SONIA NATH, Research Scholar
of Department of Law, Nagaland University, Lumami
has presented/ contributed their research paper A Socio-legal Study on the use of Digital Technology
in National Education Policy (NEP-2020)

Technical Chairperson

Seminar Director
N. Kumar
Head
ICSRD
Bengaluru, Karnataka

Organizing Secretary
Dr. Abhilasha Kumari
I.Q.A.C. Co-ordinator
Kumar B.Ed. College
Dhanbad

Chairman
Promod Kumar
Director
Kumar B.Ed. College
Dhanbad

Convener
Dr. Pawan Kumar
Principal
Kumar B.Ed. College
Dhanbad



ICSSR sponsored National Seminar
on
Emergence of Bharat: Its significance,
challenges and way forward



Organised by
Heritage Foundation

In collaboration with
Dispur Law College



Date : 1st & 2nd March 2024

CERTIFICATE OF APPRECIATION

This is to certify that **Ms. Sonia Nath**, Research Scholar, Department of Law, Nagaland University, Lumami has presented a paper entitled **“Privacy Considerations in the Age of Digital Transformation in Emerging Bharat”** in the two day National Seminar on **“Emergence of Bharat: Its significance, challenges and way forward”** held in Dispur Law College.

Jaleswar Brahma
Chairman, Heritage Foundation

Dr. Swapna M Deka
Convener of the Seminar

Dr. Gargi Dutta Paul
Principal, Dispur Law College



Certificate



This is to certify that Prof./Dr./Mr./Ms. *Sonia Nath* participated/presented a paper titled *The Digital Personal Data Protection Act 2023: Balancing Data Privacy and Growth in the Digital Economy* at the International Conference on "Rethinking Economic Development in India: Sustainability, Livelihood and Efficiency", organized by the Department of Economics, Nagaland University in collaboration with Nagaland Economic Association (NEA), Nagaland during 12th -13th October 2023.

Prof. Jagadish K Patnaik
Vice-Chancellor

Prof. B. Kilangla Jamir
Convener

Dr. Renbeni Kikon
Organizing Secretary

International Seminar on Accounting, Finance, Business, and Social Sciences (ISAFBS'2023)
14th, 15th & 16th September 2023



DEPT. OF BUSINESS ADMINISTRATION
(ISO-21001 CERTIFIED)
ASSAM UNIVERSITY, SILCHAR (INDIA)



College of Business and Public Affairs,
(AACSB-Accredited)
Alabama A&M University, USA



DEPT. OF MANAGEMENT
NORTH EASTERN HILL UNIVERSITY,
SHILLONG (INDIA)

CERTIFICATE OF PAPER PRESENTATION

THIS CERTIFICATE IS AWARDED TO

Ms. Sonia Nath

OF NAGALAND UNIVERSITY, LUMAM, INDIA

FOR PRESENTING THE PAPER "DATA PRIVACY AND CORPORATE GOVERNANCE: A STUDY IN
THE LIGHT OF DATA PROTECTION LAWS IN INDIA"

DR. H. S. LASKAR,
SEMINAR CO-ORDINATOR,
DEPT. OF BUSINESS ADMINISTRATION,
ASSAM UNIVERSITY SILCHAR (INDIA)

PROF. ARGHO VAN DHA TACHHANG,
SEMINAR DIRECTOR & HOST,
DEPT. OF MANAGEMENT,
NORTH EASTERN HILL UNIVERSITY, SHILLONG (INDIA)

PROF. ARUP KISHAN,
SEMINAR DIRECTOR & HOST,
DEPT. OF BUSINESS ADMINISTRATION,
ASSAM UNIVERSITY SILCHAR (INDIA)

PROF. BAPI BHUYAN,
SEMINAR DIRECTOR,
COLLEGE OF BUSINESS AND PUBLIC AFFAIRS,
ALABAMA A&M UNIVERSITY, USA

ANNEXURE -IX

LIST OF RMC WORKSHOPS ATTENDED

Sl no	Organized By	Theme	Date/Days	Mode
1	National Institute of Technology (NIT) Nagaland, Department of Science and Humanities, Sponsored by ICSSR	Research Methodology Courses for M.Phill/ Ph.D/ PDF Scholar in Social Sciences	3 rd - 13 th March 2024 (10 days)	Offline
2	Department of Teacher Education, Nagaland University, Kohima Campus. Sponsored by ICSSR	Research Methodology Course for Ph.D Students in Social Sciences	21 st – 2 nd March 2023 (10 Days)	Offline



NATIONAL INSTITUTE OF TECHNOLOGY NAGALAND
(An Institute of National Importance under MoE, Government of India)

Department of Science and Humanities
Chumukedima, Nagaland - 797 103

**ICSSR Sponsored Ten Day
Research Methodology Course (RMC24) for M.Phil/Ph.D/PDF Scholars in Social Sciences**

Certificate of Participation

This is to certify that Miss. Sonia Nath
was a **Participant** in the **ICSSR Sponsored Ten Day Research Methodology Course (RMC24) for M.Phil/Ph.D/PDF Scholars in Social Sciences** held from 04-03-2024 to 13-03-2024 organised by the National Institute of Technology Nagaland, Department of Science and Humanities in collaboration with Indian Institute of Technology Guwahati, Department of Humanities and Social Sciences.

Dr. A. Wati Walling
Course Director
Associate Professor

Department of Science and Humanities, NIT Nagaland

Prof. Sambit Mallick
Course Co-Director
Professor

Department of Humanities and Social Science, IIT Guwahati

Dr. Jhimli Bhattacharyya
Head of Department
Science and Humanities
NIT Nagaland



TEN DAYS WORKSHOP ON

Research Methodology Course for Ph.D. Students in Social Sciences
21st February to 2nd March 2023

Sponsored By
Indian Council of Social Science Research (ICSSR), New Delhi

Organised By
Department of Teacher Education, Nagaland University, Kohima Campus

Certificate

This is to certify that Mr./Ms. Sonia Nath of Nagaland University
has successfully completed the ten days 'Research Methodology Course for Ph.D Students in Social Sciences' organized by
Department of Teacher Education, Nagaland University, Kohima Campus from 21st February to 2nd March 2023.

(Dr. Sugendra Yadav)
Co-Course Director
(Dr. P. K. Pattnaik)
Head of the Department
(Prof. Gyanendra Nath Tiwari)
Course Director

