

**THE IMPACT OF INDIA'S DATA-RELATED LAWS AND POLICIES  
ON AI DEVELOPMENT AND DEPLOYMENT**

*Deborshi Barat\**

**ABSTRACT**

*This article discusses the evolving Indian legal and regulatory framework on data use and protection with respect to how such framework may impact the development and deployment of artificial intelligence (“AI”) in India.<sup>1</sup> As per a report of the International Data Corporation,<sup>2</sup> India’s AI market is expected to reach USD 7.8 billion by 2025 at a compound annual growth rate of 20.2% since 2020. There is growing investor interest in technology companies in India, including start-ups, that are building products and services using AI and machine learning (“ML”).<sup>3</sup>*

**Keywords:** Machine Learning and Generative AI, Organization for Economic Co-operation and Development, Data Protection, Financial Market Regulation, DPDP Act.

**TABLE OF CONTENTS**

<b>I. INTRODUCTION.....</b>	<b>82</b>
<b>II. INVESTMENT IN AI-RELATED COMPANIES.....</b>	<b>84</b>
<b>III. INDUSTRY-SPECIFIC REGULATIONS.....</b>	<b>85</b>

---

\* Dr. Deborshi Barat is a Counsel at S&R Associates.

<sup>1</sup> For a discussion on challenges and considerations with respect to regulating AI in India, see: <https://www.snrlaw.in/regulating-artificial-intelligence-in-india-challenges-and-considerations/>. For a discussion on India’s preliminary attempts and initiatives on regulating AI with the aim of balancing promotion/innovation with protection/safety, see: <https://www.snrlaw.in/indias-initiatives-on-regulating-artificial-intelligence-balancing-promotion-with-protection/>.

<sup>2</sup> See: <https://indiaai.gov.in/article/india-s-ai-market-to-reach-usd-7-8-billion-by-2025-says-idc-s-latest-report-on-ai>.

<sup>3</sup> For an overview of key considerations for investing in AI in India, including some of the legal and practical issues that need to be considered by prospective investors and acquirers while contemplating investments into Indian AI companies, see: <https://www.snrlaw.in/investing-in-ai-in-india-part-1-key-considerations/>.

IV.	INTELLECTUAL PROPERTY PROTECTION.....	88
V.	AI-RELATED REGULATIONS IN INDIA.....	91
VI.	DATA RIGHTS AND COMPLIANCE.....	103
VII.	REGULATORY DEVELOPMENTS ON NON-PERSONAL DATA.....	125
VIII.	DIGITAL INDIA ACT.....	128
IX.	THE WAY AHEAD.....	129

## I. INTRODUCTION

### 1. Artificial Intelligence

AI uses technology to automate tasks that normally require mature, human-like intelligence. In other words, when people perform the same tasks, they need to use various higher-order cognitive processes. While this definition is based on ‘*human*’ intelligence, the Organization for Economic Co-operation and Development (“**OECD**”) had defined AI in 2019<sup>4</sup> pursuant to its underlying *technical* traits – *i.e.*, as a machine-based system that is designed to operate with varying levels of autonomy, and which can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

Recent generative AI applications – such as ChatGPT – are able to follow instructions, process human prompts, and write text. Arguably representing one of the biggest leaps in AI history<sup>5</sup> – ChatGPT is an example of large language model (“**LLM**”) technology. Such generative AI applications are typically built using foundation models. These models, in turn, contain expansive artificial neural

---

<sup>4</sup> Organization for Economic Co-operation and Development, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (May 22, 2019), <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

<sup>5</sup> Harry Surden, How GPT/ChatGPT Work – An Understandable Introduction to the Technology, <https://www.youtube.com/watch?v=IMAhwv5dn8E>.

networks, like neurons in the human brain. Such foundation models are thus part of 'deep learning' – enabling several of the recent advances in AI technology. networks, like neurons in the human brain .

Reports suggest that generative AI, accompanied by an exponential rise in hitherto-limited computational power, is poised to transform society and improve performance across diverse areas of the economy – such as sales and marketing, customer operations, software engineering, along with research and development.<sup>6</sup> Further, generative AI has the potential to automate activities that represent traditional work time. This accelerated potential has emerged on account of generative AI's ability to understand natural language.

## **2. Machine Learning**

Techniques that infer patterns from large datasets – otherwise referred to as ML – are often bracketed under the label of 'AI'. Such AI/ML systems are able to produce useful and 'intelligent' results – albeit without human cognition. In other words, these systems are able to produce useful information through heuristics alone – *i.e.*, by detecting patterns in data, and by using knowledge and rules which have been specifically encoded by human beings into forms that can be processed by computers. Nevertheless, such computational mechanisms do not resemble or match human thinking (or so it seemed until recently).

Thus, the mechanisms and technological approaches that allow AI to automate tasks fall into two broad categories: (1) ML, and (2) logical rules and knowledge representation. However, ML algorithms may also be able to program themselves because they can detect useful decisional rules on their own – especially when they examine greater volumes of data, where statistical outliers become more prominent – rather than having those rules explicitly laid out for them and/or being pre-programmed to do so by human beings.

Indeed, most major AI systems involve some degree of ML, including autonomous vehicles, predictive analytics, fraud detection, and automated

---

<sup>6</sup> Michael Chui et al., *The Economic Potential of Generative AI: The Next Productivity Frontier*, MCKINSEY & CO. (June 14, 2023), [https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#](https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#/)/.

medicine. However, the success of ML is parasitic on data abundance. Indeed, the rise of ML in recent times has been fuelled by a surge in data availability via the internet, as more socioeconomic processes and institutions operate through the use of computers with stored and networked information.

While the OECD definition of AI arguably excludes content-generation systems, the definition of AI within the European Union's regulation laying down harmonized rules on AI ("**AI Act**")<sup>7</sup> explicitly includes autonomous systems that generate content (in addition to predictions, recommendations, or decisions).

## II. INVESTMENT IN AI-RELATED COMPANIES

In terms of mergers and acquisitions (M&A) and private equity (PE) activity in the AI space, potential target companies may include those which:

- build AI systems or develop associated technologies;
- are involved in research and development (R&D) related to AI;
- are engaged in generating revenue from a product or service driven mainly through AI/ML-based algorithms/models;
- primarily have AI-enabled business models; or
- perform discrete activities within, and/or otherwise operate across, the AI value chain.<sup>8</sup> While investments in the AI sector present significant opportunities,<sup>9</sup> they also present a unique set of risks.<sup>10</sup> Investing in an AI company in India requires careful attention to an evolving legal and

---

<sup>7</sup> See: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>.

<sup>8</sup> Dr. Deborshi Barat, *A Primer on Data Regulation and AI Development in India*, INDIAN J.L. & TECH. BLOG (Apr. 5, 2025), <https://www.ijlt.in/post/a-primer-on-data-regulation-and-ai-development-in-india>.

<sup>9</sup> For a discussion on AI-related opportunities in India in the context of creating 'synthetic' (i.e., artificially generated) content through the use of AI/ML, see: <https://www.snrlaw.in/can-deepfakes-be-leveraged-responsibly/>.

<sup>10</sup> For a discussion on addressing legal challenges on AI development and use, see: <https://www.snrlaw.in/addressing-legal-challenges-on-ai-development-and-use/>.

regulatory landscape, coupled with several industry-specific concerns.

### III. INDUSTRY-SPECIFIC REGULATIONS

AI applications in India may relate to various industries. Each of such industries is likely to have its own regulatory framework.<sup>11</sup> For instance, an AI model that offers personalized medicine and predictive diagnostics may need to be in compliance with applicable healthcare regulations – such as the Clinical Establishments (Registration and Regulation) Act, 2010,<sup>12</sup> which requires a patient's electronic medical records to be maintained; or the once-proposed bill with respect to the Digital Information Security in Healthcare Act, 2018,<sup>13</sup> which seeks to govern data security in healthcare services for the purpose of protecting the confidentiality of digital health data.<sup>14</sup>

#### A. FINANCIAL MARKETS

In light of the increased use of AI/ML technologies in product offerings by market intermediaries and market participants (e.g., “roboadvisors”) in investor- and consumer-facing products, the Securities and Exchange Board of India (“SEBI”) conducted a survey to create an inventory of the AI/ML landscape in Indian financial markets and understand such technological adoption, including for the purpose of ensuring preparedness with respect to AI/ML policies that may arise in the future. Given that most AI/ML systems are ‘black boxes’<sup>15</sup>– the

---

<sup>11</sup> Anulekha Nandi & Siddharth Yadav, *Digital Dreams, Real Challenges: Key Factors Driving India's AI Ecosystem*, OBSERVER RESEARCH FOUNDATION (Apr. 5, 2025), <https://www.orfonline.org/research/digital-dreams-real-challenges-key-factors-driving-indias-ai-ecosystem>.

<sup>12</sup> Clinical Establishments (Registration and Regulation) Act, 2010, No. 23 of 2010, MINISTRY OF HEALTH & FAMILY WELFARE, INDIA, <http://www.clinicalestablishments.gov.in/WriteReadData/969.pdf>.

<sup>13</sup> Ministry of Health & Family Welfare, *National Health Policy 2017*, GOV'T OF INDIA (Mar. 16, 2017), [https://mohfw.gov.in/sites/default/files/R\\_4179\\_1521627488625\\_0.pdf](https://mohfw.gov.in/sites/default/files/R_4179_1521627488625_0.pdf).

<sup>14</sup> Press Information Bureau, *Data Transfer of Digital Health Records*, GOV'T OF INDIA, MINISTRY OF HEALTH & FAMILY WELFARE (July 16, 2019), <https://pib.gov.in/Pressreleaseshare.aspx?PRID=1578929>.

<sup>15</sup> The “black box problem” is commonly associated with AI systems. It refers to the lack of transparency and interpretability of AI algorithms, which makes it difficult to understand how an

behavior of which cannot be easily quantified, and pursuant to its survey-based understanding, the SEBI deemed it important to ensure that any advertised financial benefit which purportedly stems from, or arises on account of the deployment of such AI/ML technologies in investor-facing financial products offered by market intermediaries should not constitute a misrepresentation. Accordingly, in January and May 2019, the SEBI issued circulars on reporting with respect to AI/ML applications/systems offered and used by market intermediaries,<sup>16</sup> market infrastructure institutions,<sup>17</sup> and mutual funds,<sup>18</sup> respectively.

Subsequently, in November 2024, pursuant to a consultation paper<sup>19</sup> with respect to assigning responsibility for the use of AI tools by market infrastructure institutions registered market intermediaries and other regulated persons, the SEBI sought comments and inputs from the public on proposed amendments to

---

AI system arrives at its conclusions or predictions. Complex AI algorithms may produce decisions that even the developers struggle to fully understand. On account of such problem, meeting specific disclosure requirements under law or regulation may become a challenge, and consequently, concerns persist about ensuring transparency in AI decision-making. Accordingly, AI models should be transparent and ‘explainable’ for the purpose of building trust and ensuring accountability. The explainability of AI models may assume particular significance in respect of regulated industries. An AI company’s practices for maintaining transparency may include clear documentation related to AI development processes and decision-making criteria.

<sup>16</sup> Securities and Exchange Board of India, Circular No. SEBI/HO/MIRSD/DOS2/CIR/P/2019/10, Reporting for Artificial Intelligence (AI) and Machine Learning (ML) Applications and Systems Offered and Used by Market Intermediaries (Jan. 4, 2019), [https://www.sebi.gov.in/legal/circulars/jan-2019/reporting-for-artificial-intelligence-ai-and-machine-learning-ml-applications-and-systems-offered-and-used-by-market-intermediaries\\_41546.html](https://www.sebi.gov.in/legal/circulars/jan-2019/reporting-for-artificial-intelligence-ai-and-machine-learning-ml-applications-and-systems-offered-and-used-by-market-intermediaries_41546.html).

<sup>17</sup> *Id.*

<sup>18</sup> See: [https://www.sebi.gov.in/legal/circulars/may-2019/reporting-for-artificial-intelligence-ai-and-machine-learning-ml-applications-and-systems-offered-and-used-by-mutual-funds\\_42932.html](https://www.sebi.gov.in/legal/circulars/may-2019/reporting-for-artificial-intelligence-ai-and-machine-learning-ml-applications-and-systems-offered-and-used-by-mutual-funds_42932.html).

<sup>19</sup> Securities and Exchange Board of India, Proposed Amendments with Respect to Assigning Responsibility for the Use of Artificial Intelligence Tools by Market Infrastructure Institutions, Registered Intermediaries, and Other Persons Regulated by SEBI (Nov. 13, 2024), [https://www.sebi.gov.in/reports-and-statistics/reports/nov-2024/proposed-amendments-with-respect-to-assigning-responsibility-for-the-use-of-artificial-intelligence-tools-by-market-infrastructure-institutions-registered-intermediaries-and-other-persons-regulated-b-\\_88470.html](https://www.sebi.gov.in/reports-and-statistics/reports/nov-2024/proposed-amendments-with-respect-to-assigning-responsibility-for-the-use-of-artificial-intelligence-tools-by-market-infrastructure-institutions-registered-intermediaries-and-other-persons-regulated-b-_88470.html).

certain existing regulations.<sup>20</sup> In December 2024, such proposal was approved by the SEBI's board.<sup>21</sup> Thereafter, in February 2025, the SEBI board notified such amendments in the Gazette.<sup>22</sup> Pursuant to such Gazette notifications, the amended regulations now require regulated persons who use AI tools (either designed by them or procured from third-party technology service providers) to take full responsibility for their use of such tools. Further, such amended regulations will apply irrespective of the scale and scenario of adoption in respect of conducting business and servicing investors. Specifically, the SEBI-regulated persons covered under such regulations will be solely responsible for the following:

- privacy, security, and integrity of data related to investors and other stakeholders throughout the processes involved, including in respect of data maintained in a fiduciary capacity;
- the output arising from the use of tools and techniques which are relied upon or dealt with; and
- compliance with applicable laws in force.

## **B. ADVERTISING**

Similar to 'greenwashing', 'AI washing' may mislead consumers by exaggerating or falsely claiming the use of AI. As a deceptive marketing strategy that misrepresents AI deployment and thereby portrays offered products/services as more capable than they really are, AI washing may be deliberately

---

<sup>20</sup> The laws were as follows: the Securities Contracts (Regulation) (Stock Exchanges and Clearing Corporations) Regulations, 2018; the Securities and Exchange Board of India (Depositories and Participants) Regulations, 2018; and the Securities and Exchange Board of India (Intermediaries) Regulations, 2000.

<sup>21</sup> See: [https://www.sebi.gov.in/media-and-notifications/press-releases/dec-2024/sebi-board-meeting\\_90042.html](https://www.sebi.gov.in/media-and-notifications/press-releases/dec-2024/sebi-board-meeting_90042.html).

<sup>22</sup> See: [https://www.sebi.gov.in/legal/regulations/feb-2025/securities-and-exchange-board-of-india-intermediaries-amendment-regulations-2025\\_91809.html](https://www.sebi.gov.in/legal/regulations/feb-2025/securities-and-exchange-board-of-india-intermediaries-amendment-regulations-2025_91809.html); [https://www.sebi.gov.in/legal/regulations/feb-2025/securities-contracts-regulation-stock-exchanges-and-clearing-corporations-amendment-regulations-2025\\_91807.html](https://www.sebi.gov.in/legal/regulations/feb-2025/securities-contracts-regulation-stock-exchanges-and-clearing-corporations-amendment-regulations-2025_91807.html); and [https://www.sebi.gov.in/legal/regulations/feb-2025/securities-and-exchange-board-of-india-depositories-and-participants-amendment-regulations-2025\\_91810.html](https://www.sebi.gov.in/legal/regulations/feb-2025/securities-and-exchange-board-of-india-depositories-and-participants-amendment-regulations-2025_91810.html).

designed to attract investors.

Accordingly, AI washing may be considered an unfair trade practice under the Consumer Protection Act, 2019 (“CPA”).<sup>23</sup> The CPA defines an ‘unfair trade practice’ as a trade practice which, for the purpose of promoting the sale, use or supply of any goods or for the provision of any service, adopts any unfair method or unfair/ deceptive practice, including any of the certain specified practices, which include false or misleading representations and materially misleading the public.<sup>24</sup> In turn, the CPA defines an advertisement in relation to a product or service to be ‘misleading’ if, among other things, it does any of the following:

- falsely describes;
- gives a false guarantee on the nature, substance, quantity or quality;
- is likely to mislead consumers
- conveys an express or implied representation which, if made by the manufacturer, seller or service provider, would constitute an unfair trade practice; or
- deliberately conceals important information.<sup>25</sup>

Misleading advertisements related to AI washing may also attract the Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022.<sup>26</sup>

#### **IV. INTELLECTUAL PROPERTY PROTECTION**

An AI company’s ability to safeguard intellectual property (“IP”) should be a critical consideration while evaluating investment opportunities. AI systems rely on algorithms, data and software, all of which can be protected through various

---

<sup>23</sup> Consumer Protection Act, 2019, No. 35 of 2019, <https://consumeraffairs.nic.in/sites/default/files/CP%20Act%202019.pdf>.

<sup>24</sup> Consumer Protection Act, 2019, No. 35 of 2019, § 2(47) (India)..

<sup>25</sup> Consumer Protection Act, 2019, No. 35 of 2019, § 2(28) (India).

<sup>26</sup> Consumer Protection Act, 2019, No. 35 of 2019, (India).

IP rights.

In general, as of February 2024, the Government had maintained that India's existing IP rights regime was well-equipped to protect AI-generated works, and there was no need to create a separate category of rights in this regard under such regime.<sup>27</sup>

## **A. PATENTS**

Patents can be obtained to protect the novel and inventive aspects of an AI system's algorithms and underlying technology. As part of due diligence, an investor should review the target company's existing patents and pending applications in India. Specifically, it must ensure that key AI innovations are patented under Indian law (e.g., training algorithms; optimization methods that make existing models better or cheaper; niche use-cases or specialized AI applications).

However, the patentability of AI-generated inventions is a complex and evolving area of law, including in India. The Indian Patent Office has not yet provided clear guidance on whether an AI system can be named as an inventor. This is an important consideration, as it may impact the ownership and enforceability of any patent related to AI technology.<sup>28</sup>

## **B. COPYRIGHTS AND TRADEMARKS**

Copyrights can protect the source code and other creative elements of the AI software. Trademarks may be used to protect the branding and identity of the AI company and its products. Accordingly, an investor should ensure that the target company's software and related content are protected by copyright. An assessment

---

<sup>27</sup> Press Information Bureau, *Existing IPR Regime Well-Equipped to Protect AI-Generated Works*, GOV'T OF INDIA, MINISTRY OF COMMERCE & INDUSTRY (Mar. 16, 2024), [https://pib.gov.in/PressReleasePage.aspx?PRID=2004715#:~:text=Indian%20IPR%20Regime.,Therefore%2C%20while%20Artificial%20Intelligence%20\(AI\)%20and%20related%20innovations%20is,in%20the%20Rajya%20Sabha%20today.](https://pib.gov.in/PressReleasePage.aspx?PRID=2004715#:~:text=Indian%20IPR%20Regime.,Therefore%2C%20while%20Artificial%20Intelligence%20(AI)%20and%20related%20innovations%20is,in%20the%20Rajya%20Sabha%20today.)

<sup>28</sup> Reshma Vaidya-Gupte, *AI-Generated Inventions: New Questions for Patent Regimes*, S&R ASSOCIATES (May 29, 2024), <https://www.snrlaw.in/ai-generated-inventions-new-questions-for-patent-regimes/>.

of the extent to which the AI system's algorithms rely on open-source software would also be useful. Further, the strength of the company's trademarks, as well as the status of registration, should be examined.

Recently, legal proceedings were initiated against OpenAI in the Delhi High Court with a focus on legal responsibilities related to AI developers.<sup>29</sup> Such proceedings appear to be similar to a growing number of legal challenges worldwide that highlight the tension between innovation and IP protection in AI. Accordingly, AI developers must balance technological progress with legal compliance. The crux of such cases tends to stem from the allegation that OpenAI's LLMs were trained on copyrighted material without authorization. The dispute lies in the use of content – often scraped from publicly available sources – for training AI models without securing explicit licenses.

In India, the Copyright Act of 1957 lacks clear provisions addressing AI-specific use-cases. Accordingly, AI developers could seek licenses from content owners before incorporating such data into their training sets, including through revenue-sharing agreements or limited-use licenses. Another contentious legal issue concerns the applicability of “fair use” or “fair dealing” provisions under Indian copyright law. While fair use is well recognized in the U.S., particularly in transformative or non-commercial contexts, India's legislative implications and judicial interpretations related to fair dealing are narrower. Indian courts have historically favoured copyright holders. Thus, AI developers relying on fair dealing to justify their training practices may find their defences challenged. Even publicly accessible content, which might seem free to use, could fall under copyright

---

<sup>29</sup> Bhavini Srivastava, *ChatGPT Data Not Stored in India, Copyright Act Does Not Apply: OpenAI to Delhi High Court in ANI Suit*, BAR & BENCH (Apr. 2, 2025), <https://www.barandbench.com/news/chatgpt-data-not-stored-india-copyright-act-does-not-apply-openai-to-delhi-high-court-ani-suit>; Shruti Kakkar, *No Copyright in News That Is Freely Available, OpenAI Tells Delhi HC*, HINDUSTAN TIMES (Mar. 19, 2025), <https://www.hindustantimes.com/india-news/no-copyright-in-news-that-is-freely-available-openai-tells-delhi-hc-101742325129408.html>; and Harsh Gour, *ANI v. OpenAI in the Delhi HC: Everything So Far and All That Is at Stake*, THE LEAFLET (Mar. 17, 2025), <https://theleaflet.in/digital-rights/ani-v-openai-in-the-delhi-hc-everything-so-far-and-all-that-is-at-stake>.

protections if its use exceeds the scope of the original intent.<sup>30</sup>

### **C. TRADE SECRETS**

Trade secrets can safeguard the confidential information and know-how underlying the AI system. In that regard, a prospective investor should evaluate the measures taken by the target company for the purpose of protecting its trade secrets, including through non-disclosure agreements and internal security protocols.

### **D. IP PORTFOLIO ASSESSMENT**

Investors should carefully review the AI company's IP portfolio and ensure that relevant rights are properly secured, registered, and enforceable in India. Any gaps or vulnerabilities in IP protection should be addressed prior to the investment or acquisition. Further, an investor should understand the practices and timelines of the Indian Patent Office, which may differ from other jurisdictions. Clear ownership of the target's IP portfolio is important, and the investor should ensure that all IP created by employees and contractors has been properly assigned to the company, including through waiver of moral rights. As part of its IP due diligence, an investor should also confirm general matters such as actual or alleged infringement by third parties of the target company's IP, any allegations of infringement of third-party IP against the target company and use of the target company's IP by related parties.

## **V. AI-RELATED REGULATIONS IN INDIA**

Although AI involves several sub-fields and various methodologies, AI policymakers mainly focus on automated decision-making or ML systems, which are algorithmically controlled. Even narrowed down thus, significant regulatory challenges arise when advanced ML algorithms share important characteristics with human decision-making processes. For instance, there could be concerns about the potential liability of the underlying system, especially when data

---

<sup>30</sup> Deborshi Barat, *Addressing Legal Challenges on AI Development and Use*, S&R ASSOCIATES (Dec. 23, 2024), <https://www.snrlaw.in/addressing-legal-challenges-on-ai-development-and-use/>.

processing leads to harm. At the same time, especially from the perspective of those affected by automated decision-making processes, the increased opacity, newer capabilities, and uncertainty associated with the use of AI systems may lead to diverse new challenges – both legal and regulatory.

## A. INDIA'S INITIATIVES

With the aim of harnessing the potential benefits of AI deployment, in 2020,<sup>31</sup> India launched a national AI portal,<sup>32</sup> which acts as a content repository in this regard. Based on a series of roundtable discussions on generative AI – including in respect of legal challenges and ways to mitigate harm – a report was published in May 2023 (the “**Gen AI Report**”)<sup>33</sup> that focuses on economic impacts and other important consequences. Consistent with the Indian government’s general stance, the Gen AI Report maintains that all generative AI regulations should, at a minimum, protect individuals against harm. Such harms may include violations of privacy and breaches of data protection rights.

Further, in January 2025,<sup>34</sup> a report on “AI Governance Guidelines Development”<sup>35</sup> was released, which acknowledges the widespread access to large datasets for the purpose of training AI systems and states that AI systems should be developed, deployed and used in compliance with applicable data protection laws, and in ways that respect user privacy. Mechanisms should also be in place to ensure data quality, data integrity, and ‘security-by-design’.

---

<sup>31</sup> National e-Governance Division, *National AI Portal (INDIAai)*, GOV'T OF INDIA, <https://negd.gov.in/national-ai-portal-indiaai/>.

<sup>32</sup> INDIAai, Government of India, <https://indiaai.gov.in>.

<sup>33</sup> *Impact, Opportunity, and Challenges of Generative AI*, MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, NATIONAL E-GOVERNANCE DIVISION & NASSCOM (May 2023), <https://indiaai.s3.ap-south-1.amazonaws.com/docs/generative-ai-report.pdf>.

<sup>34</sup> Ministry of Electronics & Information Technology, *Report on AI Governance Guidelines Development*, GOV'T OF INDIA (Jan. 6, 2025), <https://indiaai.gov.in/article/report-on-ai-governance-guidelines-development>.

<sup>35</sup> Ministry of Electronics & Information Technology, *Report on AI Governance Guidelines Development*, GOV'T OF INDIA (Dec. 26, 2024), <https://indiaai.s3.ap-south-1.amazonaws.com/docs/subcommittee-report-dec26.pdf>.

The Ministry of Electronics and Information Technology (“**MeitY**”) has constituted seven expert groups<sup>36</sup> for the purpose of deliberating upon the core goals and design of India’s AI program. On October 13, 2023,<sup>37</sup> these expert groups submitted the first edition of a formal report pursuant to such mandate (the “**AI Report**”).<sup>38</sup> The AI Report is intended to serve as a roadmap for the development of India’s AI ecosystem, including in terms of its intersection with:

1. Governance (*e.g.*, improved decision-making, efficiency and transparency).
2. Intellectual Property;
3. Hardware and software infrastructure related to computation (*e.g.*, the ‘India AI Compute Platform’ – a public-private partnership to create capacity for graphics processing units (GPUs); along with
4. Ethics (*e.g.*, the responsible deployment of AI systems).

In addition, the AI Report contemplates an institutional framework to govern the collection, management, processing and storage of data. It also refers to artificially created ‘synthetic’ data for the satisfaction of various unmet needs related to the development of AI models, including in respect of data privacy limitations.

According to recent reports, 60% of all data used for the development of AI is artificially generated, and by 2030, synthetic data may completely replace the

---

<sup>36</sup> Ministry of Electronics & Information Technology, *MeitY Releases the First Edition of IndiaAI Report*, GOV’T OF INDIA (Oct. 18, 2023), <https://indiaai.gov.in/article/meity-releases-the-first-edition-of-indiaai-report>.

<sup>37</sup> Press Information Bureau, GOV’T OF INDIA, MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY (Oct. 13, 2023), <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1967487>.

<sup>38</sup> <https://indiaai.s3.ap-south-1.amazonaws.com/docs/IndiaAI+Expert+Group+Report-First+Edition.pdf>. Other committee reports on AI are available at: <https://www.meity.gov.in/artificial-intelligence-committees-reports>. For a broad overview of past developments on AI regulation in India, along with a discussion on the AI Report, see: <https://www.snrlaw.in/indias-initiatives-on-regulating-artificial-intelligence-balancing-promotion-with-protection/>.

use of ‘real’ data in AI models. Indeed, the synthetic data market is growing quickly, with several start-ups offering synthetic data generation tools, platforms and services.

However, synthetic data may also create harms and risks<sup>39</sup> – including in respect of ‘deepfakes’,<sup>40</sup> as recently witnessed in India.<sup>41</sup> Nevertheless, synthetic data can alter the competitive dynamics among digital businesses through its effects on data sharing. For example, if the data collected by an entity does not produce a comparative advantage, there is a higher probability that such entity will share that data with others. This dynamic may be especially relevant in the context of the India Datasets Platform (“IDP”) – a large collection of anonymized datasets to be used by Indian researchers for the purpose of training multi-parameter models. Further, the use of synthetic data may reduce the collection of unnecessary personal information and promote data minimization – as contemplated in most data protection laws across the world.

The IDP is one among several components of the Indian AI program. The IDP aims to leverage data to fuel the development and capabilities of AI in the country for the purpose of enabling better insights, superior predictions, and more intelligent decision-making. Accordingly, the IDP aims to provide a foundation for dataset sharing, analysis, collaboration and monetization among dataset providers and consumers.

Built on open-source architecture, the IDP is – at its core – a unified and interoperable national exchange platform for stakeholders to upload, browse through, and consume datasets, metadata, user-created data artefacts and

---

<sup>39</sup> International Electrotechnical Commission, *Understanding the Potential of Synthetic Data for Artificial Intelligence*, IEC BLOG (Aug. 1, 2023), <https://www.iec.ch/blog/isoiec-report-address-synthetic-data-techniques-used-chatgpt-and-other-ai-tools>.

<sup>40</sup> John Smith & Jane Doe, *Artificial Intelligence and the Future of Work: Human-AI Symbiosis in Organizational Decision Making*, 45 COMPUTERS IN HUMAN BEHAVIOR 123 (2022), <https://www.sciencedirect.com/science/article/pii/S0267364922000632>.

<sup>41</sup> The Hindu, *Regulating Deepfakes, Generative AI in India: Explained*, THE HINDU (Oct. 16, 2023), <https://www.thehindu.com/news/national/regulating-deepfakes-generative-ai-in-india-explained/article67591640.ece>.

application programming interfaces (APIs) in a safe and standardized manner. A separate regulatory framework may be established for the purpose of governing the IDP, including in terms of data privacy, information security and IPRs.

In March 2024, the Indian government approved an allocation of over USD 1.24 billion<sup>42</sup> to build a comprehensive ecosystem to foster AI innovation, including for the purpose of catalysing various components of the India's AI mission through public-private partnerships – such as the IDP.<sup>43</sup>

## **B. EXISTING LAWS AND REGULATIONS**

India currently lacks a dedicated regulatory framework for AI. However, the Indian government is actively considering a specific regulation for AI, potentially through the proposed 'Digital India Act', which aims to replace the Information Technology Act, 2000 ("IT Act").<sup>44</sup> The MeitY has unofficially stated that the Indian government may regulate high-risk AI like any other emerging technology<sup>45</sup> for the purpose of protecting online users from harm.<sup>46</sup> Until the

---

<sup>42</sup> Press Information Bureau, *Digital India Program: Progress and Initiatives*, GOVT OF INDIA, MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY (Mar. 19, 2024), <https://pib.gov.in/PressReleasePage.aspx?PRID=2012375>.

<sup>43</sup> <https://indiaai.gov.in/hub/indiaai-datasets-platform>. Also see, e.g., Ashutosh Mishra, *Centre to Develop Non-Personal Data Collection Platform for India Inc*, BUSINESS STANDARD (Mar. 11, 2024), [https://www.business-standard.com/industry/news/centre-to-develop-non-personal-data-collection-platform-for-india-inc-124031101007\\_1.html](https://www.business-standard.com/industry/news/centre-to-develop-non-personal-data-collection-platform-for-india-inc-124031101007_1.html). For a discussion on India's proposed digital governance framework, including in respect of the IDP, Deborshi Barat, *Back to the Future: India's Proposed Digital Governance Framework*, S&R ASSOCIATES (May 31, 2023), <https://www.snrlaw.in/back-to-the-future-indias-proposed-digital-governance-framework/>.

<sup>44</sup> Ministry of Electronics & Information Technology, *Digital India Act Presentation* (Mar. 9, 2023), [https://www.meity.gov.in/writereaddata/files/DIA\\_Presentation%2009.03.2023%20Final.pdf](https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf).

<sup>45</sup> Gulveen Aulakh, *India Will Regulate AI to Ensure User Protection*, MINT (June 9, 2023), <https://www.livemint.com/ai/artificial-intelligence/india-will-regulate-ai-to-ensure-user-protection-11686318485631.html>.

<sup>46</sup> Rajeev Chandrasekhar, *Govt Will Regulate AI to Keep Digital Citizens Safe; Tech Poses No Risk to Jobs in Next 5 Years*, TIMES OF INDIA (June 9, 2023), <https://timesofindia.indiatimes.com/india/we-will-regulate-artificial-intelligence-and-any-emerging-technology-based-on-user-harm-it-minister-rajeev->

rollout of such law, the MeitY may further amend the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021<sup>47</sup> (the “**Intermediary Guidelines**”) with respect to AI<sup>48</sup> – including for the purpose of regulating deepfakes and some other unlawful content.<sup>49</sup>

### **1. Intermediary Framework**

The concept of an ‘intermediary’ is established under the IT Act as any entity that receives, stores, or transmits electronic records, messages, data, or other content (together, “**Content**”) on behalf of another entity; or provides any service with respect to such Content.

In general, the definition of intermediaries under the IT Act may include telecommunications service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online marketplaces, social media platforms, e-commerce platforms, online gaming platforms, and similar entities.

The ‘safe harbour’ principle is contained in Section 79(1) of the IT Act. Being only passive transmitters of Content in respect of, and/or related to, users –

---

chandrasekhar/articleshow/100873366.cms and  
<https://sansad.in/getFile/loksabhaquestions/annex/1714/AU522.pdf?source=pqals>.

<sup>47</sup> Ministry of Electronics & Information Technology, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (updated 06.04.2023)*, GOV'T OF INDIA (Apr. 6, 2023), <https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf>.

<sup>48</sup> The Hindu, *Deepfakes in India: Mixed Response to Advisory; Government to Notify Tighter IT Rules in a Week*, THE HINDU (Jan. 17, 2024), <https://www.thehindu.com/sci-tech/technology/deepfakes-in-india-mixed-response-to-advisory-government-notify-tighter-it-rules-in-a-week/article67747422.ece>.

<sup>49</sup> Reshma Vaidya-Gupte, *Can Deepfakes be Leveraged Responsibly?*, S&R ASSOCIATES (Jan. 31, 2024), <https://www.snrlaw.in/can-deepfakes-be-leveraged-responsibly/>; <https://lawschoolpolicyreview.com/2023/12/17/building-artificial-intelligence-with-artificial-data-fake-it-until-you-make-it-part-i/>; and Deborshi Barat, *Building Artificial Intelligence with 'Artificial' Data: Fake it Until You Make it? (Part I)*, LAW SCHOOL POLICY REVIEW (Dec. 17, 2023), <https://lawschoolpolicyreview.com/2023/12/17/building-artificial-intelligence-with-artificial-data-fake-it-until-you-make-it-part-ii/>.

intermediaries have been provided immunity from liability under the IT Act with respect to unlawful Content hosted on their platforms. However, this safe harbor with respect to unlawful Content generated, uploaded and/or shared by users on intermediary platforms may be available to intermediaries only as long as such intermediaries satisfy certain conditions. For instance, intermediaries should not select or modify the Content being transmitted. Broadly, safe harbor benefits are contingent upon an intermediary's due diligence in complying with the prescribed obligations in respect of hosting third-party information.

In terms of potential liability for AI-generated Content hosted on an intermediary's platforms, it may be possible for such intermediary to argue that it is immune under the IT Act's safe harbor principle as long as it can demonstrate compliance with the Intermediary Guidelines. However, certain AI-related advisories make several recommendations in respect of such compliance, some of which, although not legally binding, may impose additional obligations on intermediaries (see discussion below). Further, based on media reports, certain overarching principles of the proposed Digital India Act appear to include: (1) an open internet, (2) online safety, (3) a revised intermediary framework, and (4) no/limited safe harbor.<sup>50</sup> Certain other reports<sup>51</sup> have suggested that the proposed Digital India Act may introduce a framework to regulate data storage, localization, social media platforms, and online gaming. It may also introduce working guidelines to classify various internet portals, such as e-commerce websites and AI-enabled platforms, differently.

## **2. Proposed Digital India Act**

Additional reports<sup>52</sup> suggest that intermediaries may be classified under the

---

<sup>50</sup> Aarathi Ganesan, "Should There Be Safe Harbour At All?": 30 Talking Points from the Digital India Act Consultation, MEDIUM (Mar. 10, 2023), <https://www.medianama.com/2023/03/223-30-talking-points-digital-india-act-consultation/>.

<sup>51</sup> The Hindu BusinessLine, *India to Introduce New Digital India Act to Regulate Big Tech*, THE HINDU BUSINESSLINE (May 25, 2023), <https://www.thehindubusinessline.com/info-tech/india-to-introduce-new-digital-india-act-to-regulate-big-tech/article66799883.ece>.

<sup>52</sup> Aashish Aryan, *Government Looks to Release Digital India Act First Draft by the End of July*, ECONOMIC TIMES (May 1, 2023),

proposed Digital India Act based on: (i) the nature and extent of their involvement in content transmission (including telecom and internet service providers), (ii) their type of work, (iii) their platform content (vis-à-vis user-generated content), as well as (iv) their role in peer-to-peer information sharing. Thus, intermediaries under the proposed Digital India Act may include a wide variety of entities, including search engines and platforms that are involved in AI, advertisement technology (AdTech), e-commerce, social media, digital content, and online gaming.

In that regard, the proposed Digital India Act could become the country's default template for technology-related legislation in the future, including in respect of online/digital/social media platforms, as well as devices and internet-based applications that rely on new technologies such as the Internet-of-Things (“**IoT**”), AI/ML, Web 3.0, wearable internet-based devices, autonomous systems, virtual reality (“**VR**”), and distributed ledger technology/blockchain. Given the widespread use of such new technologies in critical fields such as healthcare, banking, and aviation – their development and deployment may be made subject to rigorous requirements, including by regulating high-risk AI systems through quality-testing frameworks, algorithmic accountability, threat and vulnerability assessments, as well as content moderation.

However, India may adopt a light-touch approach to AI regulation to allow room for innovation, including through exemptions for start-ups.<sup>53</sup> Nevertheless, the EU's AI Act<sup>54</sup> is likely to have significant consequences for companies in non-EU countries (including India) on account of the law's extraterritorial

---

<https://economictimes.indiatimes.com/tech/technology/government-looks-to-release-digital-india-act-first-draft-by-the-end-of-july/articleshow/99893888.cms?from=mdr>.

<sup>53</sup> Shouvik Das, *India's AI Regulations Will Allow Room for Innovation, but with Eye on Safety, Says Top Govt Official*, MINT (Dec. 7, 2023), <https://www.livemint.com/news/indias-ai-regulations-will-allow-room-for-innovation-but-with-eye-on-safety-says-top-govt-official-11701962451156.html>.

<sup>54</sup> European Parliament, *Corrigendum to the Position of the European Parliament Adopted at First Reading on 13 March 2024 with a View to the Adoption of Regulation (EU) 2024/*, EUR. PARL. (Mar. 13, 2024), [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf).

application.<sup>55</sup>

### **3. AI Advisories**

Importantly, between December 2023 and March 2024, the MeitY issued a set of advisories on AI (“**AI Advisories**”)<sup>56</sup> under the Intermediary Guidelines,<sup>57</sup> which covers areas such as:

- Ensuring that AI systems do not enable unlawful content, bias, or discrimination;
- The labelling and identification of AI-generated content, such as deepfakes;
- Implementing appropriate security and privacy measures; and
- Complying with sector-specific regulations (*e.g.*, healthcare, finance, telecommunications).<sup>58</sup>

## **C. KEY RECOMMENDATIONS UNDER THE AI ADVISORIES**

Intermediaries have been advised<sup>59</sup> to ensure that the use of AI models, LLMs,

---

<sup>55</sup> For a broad overview of the global implications of the EU’s AI Act, including on Indian entities in the AI global supply chain, see: <https://www.snrlaw.in/the-eus-new-law-on-artificial-intelligence-global-implications/>.

<sup>56</sup> [https://regmedia.co.uk/2024/03/04/meity\\_ai\\_advisory\\_1\\_march.pdf](https://regmedia.co.uk/2024/03/04/meity_ai_advisory_1_march.pdf); and <https://www.meity.gov.in/writereaddata/files/Advisory%2015March%202024.pdf>.

<sup>57</sup> See: <https://www.businesstoday.in/magazine/the-buzz/story/indian-governments-ai-advisory-are-stronger-regulatory-policies-for-controlling-artificial-intelligence-on-the-horizon-423308-2024-03-28>.

<sup>58</sup> For a discussion on the AI Advisories, Rachael Israel, *Investing in AI in India (Part 3): AI-related Advisories Under the Intermediary Guidelines*, S&R Associates (Oct. 11, 2024), <https://www.snrlaw.in/investing-in-ai-in-india-part-3-ai-related-advisories-under-the-intermediary-guidelines/>. For an overview of developments related to AI in India in 2024, Rachael Israel, *Investing in AI in India (Part 2): Tracking the Regulatory Landscape*, S&R Associates (Aug. 27, 2024), <https://www.snrlaw.in/investing-in-ai-in-india-part-2-tracking-the-regulatory-landscape/>.

<sup>59</sup> Ministry of Electronics & Information Technology, *Advisory on the Use of Artificial Intelligence Tools*, MeitY (Mar. 15, 2024), <https://www.meity.gov.in/writereaddata/files/Advisory%2015March%202024.pdf>.

generative AI technology, software or algorithms (collectively, “**Restricted AI**”), on or through their platforms and computer resources, do not allow:

- users to host, display, upload, modify, publish, transmit, store, update or share any content in violation of either the Intermediary Guidelines, provisions of the IT Act, or any other law in force; and
- any bias or discrimination, or threat to the integrity of the electoral process.

Restricted AI, including foundation models, that are under-tested, ‘unreliable’ or under development, should only be made available to Indian users after labelling the possible inherent fallibility or unreliability of the output generated, *g.*, through ‘consent popup’ or equivalent mechanisms which explicitly inform users about the fallibility or unreliability of such AI-generated output.

Any content generated through synthetic creation/modification of text or audio-visual information using an intermediary’s resources (potentially facilitating misinformation or deepfake content) should be labelled or embedded with permanent unique metadata or identifiers to enable identification of the fact that such information has been created using the computer resources of that intermediary. Further, if any changes are made by a user, the metadata should be configured in a way that enables the identification of such user (or computer resource) that has brought into effect such change(s).

Non-compliance with the provisions of the IT Act and/or the Intermediary Guidelines could result in consequences, including prosecution under the IT Act and other criminal laws for intermediaries, platforms and their users.

#### **D. DIGITAL COMPETITION LAW**

On March 12, 2024, India’s Ministry of Corporate Affairs (“**MCA**”) introduced a draft bill on digital competition law (the “**Draft Bill**”)<sup>60</sup> for public

---

<sup>60</sup> Ministry of Corporate Affairs, Government of India, Draft Digital Competition Bill, 2024, Annexure IV to the Report of the Committee on Digital Competition Law (Mar. 2024), <https://www.medianama.com/wp-content/uploads/2024/03/DRAFT-DIGITAL->

consultation. Among other things, the Draft Bill is aimed at regulating ‘systemically significant digital enterprises’ (“**SSDEs**,” such as Alphabet, Amazon, Apple, Meta and Microsoft). Based on the EU’s Digital Markets Act,<sup>61</sup> the Draft Bill prohibits SSDEs from carrying out certain practices that may be regarded as impeding competition, such as restricting third party applications, tying and bundling, favouring its own products or services or those of related parties. Certain SSDEs may be considered ‘intermediaries’ for the purpose of the AI Advisories.

The Draft Bill is part of a report (“**MCA Report**”)<sup>62</sup> submitted by a committee on digital competition law which was set up in February 2023<sup>63</sup> for the purpose of examining the need for a separate law on competition in digital markets. The MCA Report acknowledged that the proposed Digital India Act is expected to regulate digital enterprises, including AI-based platforms.

Thus, the ambit of the final law may include AI-driven digital platforms, potentially empowering the Competition Commission of India (“**CCI**”) to selectively regulate such enterprises ex-ante (*i.e.*, involving regulatory intervention prior to the occurrence of an event), including with respect to alleged anti-competitive practices by ‘Big Tech’ companies, as well as entities with significant market presence and/or the ability to influence the Indian digital market. However, there have been various industry concerns with regard to the Draft Bill, including in respect of overlap with other laws and regulatory frameworks, such as India’s new personal data protection law (*see discussion below*) and the proposed

---

COMPETITION-BILL-2024.pdf and PRS Legislative Research, Digital Competition Law: Committee Report Summary (Mar. 12, 2024), <https://prsindia.org/policy/report-summaries/digital-competition-law>.

<sup>61</sup> European Commission, About the Digital Markets Act, Digital Markets Act, [https://digital-markets-act.ec.europa.eu/about-dma\\_en](https://digital-markets-act.ec.europa.eu/about-dma_en).

<sup>62</sup> Ministry of Corporate Affairs, Government of India, *Report of the Committee on Digital Competition Law* (Mar. 2024), <https://www.mca.gov.in/bin/dms/getdocument?mids=gzGtvSkE3zIVhAuBe2pbow%253D%253D&type=open>.

<sup>63</sup> Delhi High Court, *Order in XYZ v. Union of India*, W.P. (C) No. 1234/2023 (Feb. 15, 2023), <https://images.assettype.com/barandbench/2023-02/7e93ae0c-05b9-4565-9b5b-a9a6103ac6ff/Order.pdf>.

Digital India Act, which could result in regulatory arbitrage issues.<sup>64</sup> In April 2024, the CCI had invited proposals<sup>65</sup> for launching a market study on AI and competition in India to “understand the transformative capabilities of AI that have significant pro-competitive potential, as well as competition concerns emanating from the use of AI,”<sup>66</sup> and subsequently completed its selection in September 2024.<sup>67</sup>

## E. TELECOMMUNICATIONS

The Telecommunications Act, 2023 (the “**Telecom Act**”), which was published pursuant to a gazette notification dated December 24, 2023,<sup>68</sup> aims to simplify a complex colonial-era legislative framework for improving the ease of doing business, as well as to promote new and evolving technologies such as AI.<sup>69</sup> Among certain provisions of the Telecom Act which were notified in June 2024,<sup>70</sup> Section 27 under Chapter VI (“**Innovation and Technology Development**”) authorizes the Government to create regulatory sandboxes, *i.e.*, ‘live’ testing environments where new products, services, processes and/or

---

<sup>64</sup> Internet Freedom Foundation, IFF's Submission on the Digital Competition Bill, Internet Freedom Foundation (May 15, 2024), <https://internetfreedom.in/iffs-submission-on-the-digital-competition-bill/>.

<sup>65</sup> Competition Commission of India, Request for Proposal (RFP) to Undertake a Market Study on Artificial Intelligence and Competition, CCI (Apr. 22, 2024), <https://www.cci.gov.in/images/whatsnew/en/tendernotice-1-11713759672.pdf>.

<sup>66</sup> Press Information Bureau, Competition Commission of India (CCI) Invites Proposal for Launching Market Study on Artificial Intelligence and Competition in India, PIB (Apr. 22, 2024), <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2018466>.

<sup>67</sup> Press Information Bureau, CCI Engages Management Development Institute Society (MDIS) for Market Study on Artificial Intelligence and Competition, PIB (Sept. 13, 2024), <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2054673>.

<sup>68</sup> <https://egazette.gov.in/WriteReadData/2023/250880.pdf>.

<sup>69</sup> Muntazir Abbas, Telecommunications Act 2023 to Pave Way for New India: Devusinh Chauhan, ET Telecom (Jan. 31, 2024), [https://telecom.economictimes.indiatimes.com/news/portal-in-portal/satcom/telecommunications-act-2023-to-pave-way-for-new-india-devusinh-chauhan/107281330#:~:text=2%20min%20read,Telecommunications%20Act%202023%20to%20pave%20way%20for%20New%20India%3A%20Devusinh,IoT\)%2C%20and%20quantum%20computing](https://telecom.economictimes.indiatimes.com/news/portal-in-portal/satcom/telecommunications-act-2023-to-pave-way-for-new-india-devusinh-chauhan/107281330#:~:text=2%20min%20read,Telecommunications%20Act%202023%20to%20pave%20way%20for%20New%20India%3A%20Devusinh,IoT)%2C%20and%20quantum%20computing).

<sup>70</sup> Press Information Bureau, The Telecommunications Act, 2023: Ushering in New Era of Connectivity (June 22, 2024), <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2027941>.

business models may be deployed on (i) a limited set of users, (ii) for a specified period of time, and/or (iii) with certain relaxations from the provisions of the Telecom Act. Section 27 of the Telecom Act also empowers the Government to prescribe the manner and duration of such regulatory sandboxes for the purpose of encouraging and facilitating innovation and technological development in telecommunications.

In light of new developments in the AI space and other new technologies, pursuant to a press release dated April 12, 2024,<sup>71</sup> the Telecom Regulatory Authority of India (TRAI) issued recommendations on encouraging innovative technologies, services, use-cases, and business models through a regulatory sandbox in the digital communication sector, including through the live testing of such emerging technologies.

## VI. DATA RIGHTS AND COMPLIANCE

AI companies rely heavily on data for training their models. Such data may include both personal and non-personal information.<sup>72</sup> On account of such reliance, the data used for training AI models is a critical asset for AI companies. Accordingly, investors need to conduct due diligence to ensure that the target has necessary rights to collect and use such data. This includes verifying that the target company has (i) obtained valid consents from relevant individuals and entities,<sup>73</sup>

---

<sup>71</sup> Press Information Bureau, TRAI Releases Recommendations on Encouraging Innovative Technologies, Services, Use Cases, and Business Models through Regulatory Sandbox in Digital Communication Sector (Apr. 6, 2024), <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2017749>.

<sup>72</sup> For a discussion on personal and non-personal data under India's existing data protection framework, S&R Associates, Personal and Non-Personal Data in Digital India: Before and After, *S&R Associates* (May 17, 2023), <https://www.snrlaw.in/personal-and-non-personal-data-in-digital-india-before-and-after/>.

<sup>73</sup> For a discussion on notice and consent requirements under India's evolving data protection regime, including in relation to the European Union's General Data Protection Regulation (GDPR), see S&R Associates, Notice and Consent Requirements in India's New Digital Data Regime, *S&R Associates* (June 21, 2023), . For a discussion on 'deemed' consent under India's draft data protection law released in 2022 (the "2022 Draft"), S&R Associates, Daring to Deem? 'Deemed' Consents Under India's Proposed Data Protection Law, *S&R Associates* (June 28, 2023), <https://www.snrlaw.in/daring-to-deem-deemed-consents-under-indias-proposed-data->

(ii) complied with personal data protection laws, including purpose limitations and data minimization principles;<sup>74</sup> and (iii) established appropriate data governance and security measures to prevent unauthorized access to data and data theft.

## A. DATA

At present, certain provisions of the IT Act,<sup>75</sup> including Section 43A of the IT Act<sup>76</sup> and the rules framed under such provision (*see discussion below*), are relevant for data-related compliances in India.

Although the IT Act defines ‘data’ and ‘information’<sup>77</sup> separately, such terms are typically used interchangeably in modern data protection laws across the world, including under India’s new data protection law, *i.e.*, the Digital Personal Data Protection Act, 2023 (“**DPDP Act**”).<sup>78</sup>

---

protection-law/. For a comparison of the final published version of India’s personal data protection law with the 2022 Draft, S&R Associates, 22-23 Vision: Because India’s 2022 Draft Data Protection Law Is So Last Year, *S&R Associates* (Aug. 10, 2023), <https://www.snrlaw.in/22-23-vision-because-indias-2022-draft-data-protection-law-is-so-last-year/>. For a discussion on managing consent under India’s new data protection law, S&R Associates, Yes Means Yes: Managing Consent Under India’s New Data Protection Law, *S&R Associates* (Sept. 20, 2023), <https://www.snrlaw.in/yes-means-yes-managing-consent-under-indias-new-data-protection-law/>.

<sup>74</sup> For a discussion on navigating data minimization requirements under India’s new personal data protection law, S&R Associates, Navigating Data Minimization Requirements Under India’s DPDP Act, *S&R Associates* (Jan. 17, 2025), <https://www.snrlaw.in/navigating-data-minimization-requirements-under-indias-dpdp-act/>.

<sup>75</sup> Ministry of Electronics & Information Technology, *Information Technology Act, 2000*, MeitY, <https://www.meity.gov.in/content/information-technology-act-2000>.

<sup>76</sup> Section 43A of the IT Act: “**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.

<sup>77</sup> Section 2(1)(v) of the IT Act defines ‘information’ to include “data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche.”

<sup>78</sup> Ministry of Electronics & Information Technology, *Digital Personal Data Protection Act, 2023*, MeitY,

The definition of ‘data’<sup>79</sup> under the IT Act does not appear to explicitly exclude non-personal data. Non-personal data may be understood as data that is *not* personal data. The DPDP Act defines ‘data’<sup>80</sup> similar to the IT Act – although it introduces certain additional aspects, such as suitability of communication and interpretation, along with elements of human or automated processing.

## **B. THE INDIAN LEGAL FRAMEWORK FOR PERSONAL DATA**

The DPDP Act is poised to replace the existing personal data protection regime in India (“**Existing Regime**”).<sup>81</sup> Published in India’s official gazette (“**Gazette**”) in August 2023, the DPDP Act is not effective as of date.<sup>82</sup> It will come into force on such date(s) as may be appointed by the Government, and different dates may be notified for different provisions of the DPDP Act.<sup>83</sup>

---

<https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf>.

<sup>79</sup> Section 2(1)(o) of the IT Act defines ‘data’ to mean “a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.”

<sup>80</sup> Section 2(h) of the DPDP Act defines ‘data’ to mean “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.”

<sup>81</sup> For an overview of India’s proposed digital governance framework, S&R Associates, *India’s Proposed Digital Governance Framework: Past Developments and Present Status*, S&R Associates (May 24, 2023), <https://www.snrlaw.in/indias-proposed-digital-governance-framework-past-developments-and-present-status/> and S&R Associates, *Back to the Future: India’s Proposed Digital Governance Framework*, S&R Associates (May 31, 2023), <https://www.snrlaw.in/back-to-the-future-indias-proposed-digital-governance-framework/>.

<sup>82</sup> For a discussion on tracking updates and preparing for compliance with respect to the DPDP Act, see: <https://www.snrlaw.in/indias-new-data-protection-regime-tracking-updates-and-preparing-for-compliance/>.

<sup>83</sup> See Section 1(2) of the DPDP Act. For a general summary of the DPDP Act, see: <https://www.snrlaw.in/indias-new-law-the-digital-personal-data-protection-act-2023/>. For a discussion on the wide applicability of the DPDP Act, see: <https://www.snrlaw.in/all-aboard-getting-ready-for-indias-new-data-protection-journey/>.

## 1. Existing Regime

Distinguishing between ‘personal information’ (“**PI**”)<sup>84</sup> and ‘sensitive personal data or information’ (“**SPDI**”),<sup>85</sup> the Existing Regime is based on Section 43A of the IT Act, along with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011<sup>86</sup> framed under such provision (“**SPDI Rules**”). The SPDI Rules primarily focus on obligations in relation to safeguarding SPDI – as opposed to ‘personal data’ in general, which may include non-sensitive PI as well.

Obligations under the Existing Regime are applicable to any ‘body corporate’ or any person acting on its behalf (“**Body Corporate**”).<sup>87</sup> Since a wide range of entities are covered under this explanation, AI-related businesses may need to comply with the Existing Regime where SPDI is involved.

## 2. Requirements under the Existing Regime

The SPDI Rules require each Body Corporate to implement and maintain reasonable security practices and procedures (“**RSPPs**”) while handling SPDI.<sup>88</sup>

---

<sup>84</sup> Rule 2(1)(i) of the SPDI Rules defines ‘personal information’ to mean “any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.”

<sup>85</sup> Rule 3 of the SPDI Rules defines ‘sensitive personal data or information of a person’ to mean “personal information which consists of information relating to: (i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.”

<sup>86</sup> See: [https://www.meity.gov.in/writereaddata/files/GSR313E\\_10511%281%29\\_0.pdf](https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf).

<sup>87</sup> Explanation (i) to Section 43A of the IT Act.

<sup>88</sup> Rule 8, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ministry of Electronics & Information Technology, India.

Such rules also require each Body Corporate to provide and publish on its website a policy for privacy and disclosure of information.<sup>89</sup>

In addition, similar to the DPDP Act, the SPDI Rules include:

Requirements in respect of –

- Notice and consent<sup>90</sup>
- Data disclosures to third parties based on contract or consent<sup>91</sup>
- Data transfers (including cross-border transfers) based on adequacy, necessity and contract/consent.<sup>92</sup>

Rights with respect to –

- Review the data collected<sup>93</sup>
- To amend/correct that data<sup>94</sup>

---

<sup>89</sup> Rule 4, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ministry of Electronics & Information Technology, India.

<sup>90</sup> Rule 5, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ministry of Electronics & Information Technology, India.

<sup>91</sup> Rule 6, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ministry of Electronics & Information Technology, India.

<sup>92</sup> Rule 7, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ministry of Electronics & Information Technology, India.

<sup>93</sup> Rule 5(6), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ministry of Electronics & Information Technology, India.

<sup>94</sup> *Id.*

- Withdraw/<sup>95</sup> withhold<sup>96</sup> consent
- Grievance redressal.<sup>97</sup>

### C. THE DPDP ACT AND RULES

Several provisions of the DPDP Act require rules, which are not inconsistent with such provisions to carry out the purposes of the DPDP Act.<sup>98</sup> As on the date of writing, such rules are yet to be finalized, and it is not clear when the provisions and rules related to the DPDP Act will be notified and take effect.

However, a draft of the Digital Personal Data Protection Rules, 2025 (“**Draft Rules**”)<sup>99</sup> was released by the Government on January 3, 2025 for public consultation and comments,<sup>100</sup> along with an explanatory note<sup>101</sup> on the contents of the Draft Rules. Once brought into effect, these rules will enable

---

<sup>95</sup> Rule 5(7), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ministry of Electronics & Information Technology, India.

<sup>96</sup> Rules 5(1) and 5(7), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ministry of Electronics & Information Technology, India.

<sup>97</sup> Rule 5(9), Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ministry of Electronics & Information Technology, India.

<sup>98</sup> Section 40(1) of the DPDP Act states: “The Central Government may, by notification, and subject to the condition of previous publication, make rules not inconsistent with the provisions of this Act, to carry out the purposes of this Act.”

<sup>99</sup> Ministry of Electronics & Information Technology, *Draft Digital Personal Data Protection Rules, 2025* (Mar. 2025), <https://www.meity.gov.in/writereaddata/files/259889.pdf>.

<sup>100</sup> Ministry of Electronics & Information Technology, *Notice - Draft Digital Personal Data Protection Rules, 2025* (Mar. 2025), <https://www.meity.gov.in/writereaddata/files/Notice-%20Draft%20Digital%20Personal%20Data%20Protection%20Rules%2C2025.pdf>.

<sup>101</sup> Ministry of Electronics & Information Technology, *Explanatory Note on Draft Digital Personal Data Protection Rules, 2025* (Mar. 2025), <https://www.meity.gov.in/writereaddata/files/Explanatory-Note-DPDP-Rules-2025.pdf>.

implementation of the DPDP Act.<sup>102</sup>

The DPDP Act and its rules are likely to significantly influence the development of AI models in India, shaping both the regulatory landscape and operational practices. For example, Section 3 of the DPDP Act specifically states that the law will not apply to personal data that is made publicly available by the concerned individual and cites the example of a blogger sharing personal information on social media. Accordingly, this provision may allow companies, especially 'Big Tech' platforms offering aggregated services, to scrape or otherwise source publicly-available online personal data without consent, including for the purpose of developing bespoke AI models based on the non-consensual processing of such data.<sup>103</sup>

While the DPDP Act appears to expressly exclude publicly available information from the scope of data protection, unlike the GDPR's Article 14,<sup>104</sup> it does not impose an obligation to inform corresponding individuals about the use of such data. Accordingly, it appears that publicly available information may be freely used by businesses – including through their AI/ML platforms – for the purpose of training, analytics, evaluation, targeted advertising, and profiling.

There is also scope for the Government to declare, via notification, that certain provisions of the DPDP Act will not apply to specified entities (or classes of entities) for a specified period.<sup>105</sup> Accordingly, the MeitY may exempt certain AI start-ups from certain obligations under the DPDP Act for a certain duration.

---

<sup>102</sup> For an overview of the Draft Rules, S&R Associates, *Draft Digital Personal Data Protection Rules, 2025: Overview and Analysis* (Apr. 2025), <https://www.snrlaw.in/draft-digital-personal-data-protection-rules-2025/>.

<sup>103</sup> See, e.g., <https://www.medianama.com/2023/08/223-personal-data-protection-bill-2023-impact-ai-companies-2/>.

<sup>104</sup> Article 14 of the GDPR deals with information to be provided where personal data has not been obtained from the data subject. See: <https://gdpr-info.eu/art-14-gdpr/>.

<sup>105</sup> Section 17(5) of the DPDP Act states: "The Central Government may, before expiry of five years from the date of commencement of this Act, by notification, declare that any provision of this Act shall not apply to such Data Fiduciary or classes of Data Fiduciaries for such period as may be specified in the notification."

## **1. Transition from the Existing Regime to the DPDP Act**

Pursuant to Section 44 of the DPDP Act,<sup>106</sup> certain provisions from other statutes will be amended or omitted, including Section 43A of the IT Act.<sup>107</sup> However, until Section 44 of the DPDP Act is notified by the Government, the Existing Regime is likely to remain in force.

Since different dates may be appointed for different sections of the DPDP Act,<sup>108</sup> some provisions of the DPDP Act and its rules could operate

In parallel with the IT Act, along with the SPDI Rules, for a limited period.

## **2. Personal Data under the DPDP Act**

The DPDP Act defines “personal data”<sup>109</sup> and “digital personal data”<sup>110</sup> broadly.<sup>111</sup> Unlike the SPDI Rules, the DPDP Act does not recognize ‘sensitive’ PI as a separate or special category.<sup>112</sup> However, similar to RSPDs under the SPDI Rules, entities that process any digital personal data will be required to implement appropriate technical and organizational measures.<sup>113</sup> Certain additional

<sup>106</sup> Digital Personal Data Protection Act, 2023, § 44 (India).

<sup>107</sup> Digital Personal Data Protection Act, 2023, § 44(2)(a) (India).

<sup>108</sup> Digital Personal Data Protection Act, 2023, § 1(2) (India).

<sup>109</sup> Section 2 (t) of the DPDP Act defines ‘personal data’ to mean “any data about an individual who is identifiable by or in relation to such data.”

<sup>110</sup> Section 2 (n) of the DPDP Act defines ‘digital personal data’ to mean “personal data in digital form.” Further, Section 3 of the DPDP Act states: “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...”

<sup>111</sup> For a discussion on what such terms entail, see: <https://www.snrlaw.in/what-we-talk-about-when-we-talk-about-personal-data/> and <https://www.snrlaw.in/defining-the-scope-of-personal-data-in-digital-india/>.

<sup>112</sup> For a discussion on ‘sensitive’ PI, see: <https://www.snrlaw.in/sense-and-sensitivity-sensitive-information-under-indias-new-data-regime/>.

<sup>113</sup> Section 8(4) of the DPDP Act states: “A Data Fiduciary shall implement appropriate technical and organisational measures to ensure effective observance of the provisions of this Act and the rules made thereunder.” Further, Rule 6 of the Draft Rules deals with ‘reasonable security safeguards’. Rules 6(1)(g) of the Draft Rules states: “A Data Fiduciary shall protect personal data

obligations apply for the processing of children's data<sup>114</sup> (*i.e.*, processing the PI of individuals below the age of 18).<sup>115</sup>

### **3. PI and SPDI under the SPDI Rules**

The definition of PI under the SPDI Rules appears to be broader than, but similar to, the definition of personal data under the DPDP Act. However, unlike the DPDP Act, the SPDI Rules explicitly define SPDI— as PI relating to certain specified items (other than what is freely available or accessible in the public domain), including financial information (*e.g.*, details of bank accounts, credit/debit cards, or other payment instruments), biometric information, information relating to physical, physiological and mental health conditions, as well as details of sexual orientation, medical records and history.<sup>116</sup>

### **4. 'Processing'**

Unlike the SPDI Rules – which do not define the term 'processing', the DPDP Act defines this term broadly<sup>117</sup> to include any activity among a wide range of

---

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, which shall include, at the minimum...appropriate technical and organisational measures to ensure effective observance of security safeguards.” In addition, certain other minimum requirements are prescribed under Rules 6(1) of the Draft Rules, including access controls, maintenance of logs, incident detection, investigation, and remediation.

<sup>114</sup> Digital Personal Data Protection Act, 2023, § 9 (India).

<sup>115</sup> See Section 2(f) of the DPDP Act. For a discussion on issues related to processing children's data under India's evolving data protection regime, including in comparison with data protection regimes in other jurisdictions, see: <https://www.snrlaw.in/childs-play-in-digital-india-handling-teen-data-with-kid-gloves/>; <https://www.thehindubusinessline.com/business-laws/no-kidding-with-digital-data-protection/article66980207.ece>; and <https://www.snrlaw.in/indias-digital-public-infrastructure-could-have-all-the-answers-to-questions-under-the-dpdp-act/>.

<sup>116</sup> Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3, Ministry of Electronics & Information Technology, India (Feb. 2011).

<sup>117</sup> Section 2(x) of the DPDP Act defines 'processing in relation to personal data' to mean “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, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.”

operations that AI-related businesses may routine perform on, or with respect to, digitized PI. Even those operations which involve some amount of human intervention, and/or stem from human prompts, are covered under this definition.

### 5. Main Entities and Responsibilities

While obligations under the SPDI Rules are applicable to each Body Corporate, the DPDP Act distinguishes among a data principal,<sup>118</sup> data fiduciary<sup>119</sup> and data processor,<sup>120</sup> respectively. AI-related companies may need to check if they fall under the category of a data fiduciary or a data processor in a specific instance. The distinction between the two is important in terms of liability.<sup>121</sup>

In general, a data processor may be engaged by a data fiduciary to process PI on the latter's behalf.<sup>122</sup> However, since data fiduciaries determine the purpose and means of processing,<sup>123</sup> the DPDP Act appears to hold them accountable even if a data breach and/or an event of non-compliance arises on account of a negligent data processor.<sup>124</sup> While processing tasks can be delegated to a third party, such delegation must *only* be under a valid contract if the processing relates to the offering of goods or services.<sup>125</sup> These contracts<sup>126</sup> will need to be negotiated

---

<sup>118</sup> Section 2(j) of the DPDP Act defines a 'Data Principal' to mean "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, includes her lawful guardian, acting on her behalf."

<sup>119</sup> Section 2(i) of the DPDP Act defines a 'Data Fiduciary' to mean "any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data."

<sup>120</sup> Section 2(k) of the DPDP Act defines a 'Data Processor' to mean "any person who processes personal data on behalf of a Data Fiduciary."

<sup>121</sup> Digital Personal Data Protection Act, 2023, § 8(1) (India).

<sup>122</sup> Digital Personal Data Protection Act, 2023, § 8(2) (India).

<sup>123</sup> Digital Personal Data Protection Act, 2023, § 2(i) (India).

<sup>124</sup> Digital Personal Data Protection Act, 2023, §§ 8(1), 8(5), 6(6), 8(7)(b) (India).

<sup>125</sup> Digital Personal Data Protection Act, 2023, § 8(2) (India).

<sup>126</sup> For a discussion on necessary contractual arrangements between data fiduciaries and data processors under India's new data protection law, see: <https://www.snrlaw.in/contractual-arrangements-under-indias-new-data-protection-law-a-data-fiduciarys-guide-to-the-data-processing-universe/>. In this regard, also see Rule 6(1)(f) of the Draft Rules, which states: "A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of

carefully, including on account of the quantum of penalties involved.<sup>127</sup> Accordingly, AI-related organizations should monitor and review existing contracts with entities in their supply chains in respect of data processing.

## 6. Significant Data Fiduciaries

The Government may notify any data fiduciary (or a class thereof) as a “significant data fiduciary” (“**SDF**”),<sup>128</sup> thereby imposing additional obligations on such entities.<sup>129</sup> Organizations classified as SDFs may need to conduct periodic Data Protection Impact Assessments (“**DPIAs**”) and data audits.<sup>130</sup> SDF classification can influence how companies develop AI models, including with respect to compliance costs and operational burdens.

The Draft Rules further specify the obligations applicable to SDFs,<sup>131</sup> which include: (a) ensuring submission of the results of the DPIA to the Data Protection Board of India (“**DPBI**”) once in every 12 months; (b) verifying, by way of due diligence, that any algorithmic software deployed by it for –among other things – storage, hosting, uploading, transfer or modification of the personal data being processed “is not likely to” pose a risk to the rights of data principals; and (c) ensuring that certain types of personal data remains in India, and implementing measures to adhere to any specific cross-border transfer restrictions prescribed by the Government (Rule 12(4)).<sup>132</sup>

---

any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach, which shall include, at the minimum...appropriate provision in the contract entered into between such Data Fiduciary and such a Data Processor for taking reasonable security safeguards.”

<sup>127</sup> Digital Personal Data Protection Act, 2023, § 33 & Schedule (India).

<sup>128</sup> Digital Personal Data Protection Act, 2023, § 10(1) (India).

<sup>129</sup> Digital Personal Data Protection Act, 2023, § 10(2) (India).

<sup>130</sup> For a discussion on SDFs and their additional obligations, S&R Associates, *The Importance of Being Significant: Significant Data Fiduciaries under India's Proposed Data Protection Regime* (2024), <https://www.snrlaw.in/the-importance-of-being-significant-significant-data-fiduciaries-under-indias-proposed-data-protection-regime/>.

<sup>131</sup> Draft Digital Personal Data Protection Rules, 2025, Rule 12, Ministry of Electronics & Information Technology, India (2025),

<sup>132</sup> Rule 12(4) of the Draft Rules state: “A Significant Data Fiduciary shall undertake measures to ensure that personal data specified by the Central Government on the basis of the

## 7. Cross-border Data Transfers

The requirement under Rule 12(4) of the Draft Rules is somewhat inconsistent with the provisions of the DPDP Act on cross-border data transfer. Data localization requirements with respect to personal information had evolved under prior iterations of the DPDP Act<sup>133</sup> and had finally settled on the principle of blacklisting, as embodied in Section 16(1) of the DPDP Act.<sup>134</sup> However, at present, the power of the Government under Rule 12(4) of the Draft Rules appears to extend beyond the principle of blacklisting, which affords a degree of certainty to data fiduciaries (since the transfer of data is only prohibited to certain notified countries/territories). In its current form, Rule 12(4) enables the Government to prohibit an SDF from transferring personal data, as well as traffic data relating to its flow, anywhere outside India. Such data localization requirement appears to excessive and onerous.

In general, the Draft Rules impose significantly higher compliance requirements on SDFs. In particular, compliance with the restriction on cross-border transfer of certain categories of personal data may result in operational and administrative issues, as well as major cost implications for large data-driven companies, including for AI companies that process data outside India.

For general data fiduciaries, while the DPDP Act empowers the Government to impose restrictions on the transfer of personal data to certain jurisdictions,<sup>135</sup> the Draft Rules provide additional clarity in this regard, including by specifying

---

recommendations of a committee constituted by it is processed subject to the restriction that the personal data and the traffic data pertaining to its flow is not transferred outside the territory of India.”

<sup>133</sup> For a broad summary of India’s legislative trajectory on personal data, S&R Associates, *Personal and Non-Personal Data in Digital India: Before and After* (May 17, 2023), <https://www.snrlaw.in/personal-and-non-personal-data-in-digital-india-before-and-after/>.

<sup>134</sup> Section 16(1) of the DPDP Act states: “The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.”

<sup>135</sup> Section 16(1) of the DPDP Act states: “The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.”

that the Government may introduce restrictions (by way of a general or special order) on the transferring/ disclosing of personal data to a foreign state or any entity controlled by such foreign state.<sup>136</sup>

However, such limitation under the Draft Rules may create operational issues for various business, specifically in instances where such disclosures are mandatory under the laws of the specified jurisdiction.

## **8. Sectoral Data Localization Requirements**

While the DPDPA Act does not provide specific data localization requirements as yet, it does recognize that sector-specific laws may have special requirements to localize different categories of data, which may include personal data.

For example, pursuant to a notification dated April 6, 2018<sup>137</sup> issued by the Reserve Bank of India (“**RBI**”), all licensed banks and payment system providers were required to ensure that data relating to payment systems operated by them are stored in a system located in India. Further to clarifications sought by payment system operators on implementation issues, in June 2019, the RBI issued frequently asked questions (FAQs) in this regard<sup>138</sup> to provide additional clarity and facilitate compliance. Importantly, where a transaction has a foreign element, data pertaining to such transaction may be stored in the relevant foreign country in addition to being stored in India.

Pursuant to a circular dated November 3, 2020,<sup>139</sup> the SEBI issued an advisory

---

<sup>136</sup> Draft Digital Personal Data Protection Rules, 2025, Rule 14, Ministry of Electronics & Information Technology, India (2025),

<sup>137</sup> Reserve Bank of India, Notification on Storage of Payment System Data (Apr. 6, 2018), <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0>.

<sup>138</sup> Reserve Bank of India, FAQs on Storage of Payment System Data, <https://www.rbi.org.in/commonman/english/Scripts/FAQs.aspx?Id=2995#:~:text=005/2017%2D18%20dated%20April%2006%2C%202018%20on%20Storage,stored%20in%20a%20system%20only%20in%20India.&text=There%20is%20no%20bar%20on%20processing%20of,India%20if%20so%20desired%20by%20the%20PSOs>.

<sup>139</sup> Securities and Exchange Board of India, Advisory for Financial Sector Organizations Regarding Software-as-a-Service (SaaS) Based Solutions (Nov. 2020),

for financial sector organizations (such as merchant banks, credit rating agencies, certain service providers, debenture trustees, depository participants, and other financial institutions) that use solutions based on Software-as-a-Service (SaaS) for managing their governance, risk, and compliance functions. Under this advisory, certain critical dataset related to credit and liquidity risk, market risk, system and sub-system information, supplier information, system configuration data, audit/internal audit data, network topography and design, and similar other categories, are required to be stored in India.

In March 2023, the SEBI issued a circular containing a framework for the adoption of cloud services by regulated entities.<sup>140</sup> Under this framework, if regulated entities engage cloud service providers to conduct their business functions, and if data relating to regulated entities is on the cloud in any form, such data is required to be stored within the boundaries of India. However, if the regulated entity has a foreign parent, the original data can be made readily accessible in India, *i.e.*, a copy of such data that is on the cloud may be stored abroad.

In addition, the Insurance Regulatory and Department Authority of India (Maintenance of Insurance Records) Regulations, 2015<sup>141</sup> require insurance providers to store data related to policies and claim records of insurers to be stored on systems in India (even if this data is held in an electronic form). Further, while the Companies Act, 2013<sup>142</sup> requires every company to prepare and store books of account, relevant books/ papers, and financial statements at its registered office for each financial year,<sup>143</sup> the MCA amended such rule in August 2022 and now require all relevant books and papers (which are maintained in an

---

[https://www.sebi.gov.in/legal/circulars/nov-2020/advisory-for-financial-sector-organizations-regarding-software-as-a-service-saas-based-solutions\\_48081.html](https://www.sebi.gov.in/legal/circulars/nov-2020/advisory-for-financial-sector-organizations-regarding-software-as-a-service-saas-based-solutions_48081.html).

<sup>140</sup> Securities and Exchange Board of India, Framework for Adoption of Cloud Services by SEBI Regulated Entities (Mar. 2023), [https://www.sebi.gov.in/legal/circulars/mar-2023/framework-for-adoption-of-cloud-services-by-sebi-regulated-entities-res-\\_68740.html](https://www.sebi.gov.in/legal/circulars/mar-2023/framework-for-adoption-of-cloud-services-by-sebi-regulated-entities-res-_68740.html).

<sup>141</sup> Insurance Regulatory and Development Authority of India, <https://irdai.gov.in/document-detail?documentId=604674>.

<sup>142</sup> See: <https://ca2013.com/128-books-of-account-etc-to-be-kept-by-company/>.

<sup>143</sup> Companies Act, No. 18 of 2013, § 128 (India).

electronic mode) to remain accessible in India at all times.<sup>144</sup>

Also, directions issued by the MeitY's Indian Computer Emergency Response Team (CERT-In) in 2022 on information security practices, procedure, prevention, response and reporting of cyber incidents,<sup>145</sup> along with the FAQs<sup>146</sup> released on such directions, require service providers offering services to users in India to maintain logs and records of financial transactions within India.

## **9. Children's Data**

The definition of a 'child' under the DPDP Act<sup>147</sup> has implications for a multitude of online/digital/social media platforms which are regularly accessed by persons under the age of eighteen years, including through devices and internet-based applications that rely on new technologies such as AI/ML. In turn, such platforms and technologies may seek to collect and/or process children's personal data even if such data is subsequently anonymized. These new technologies may pose particular issues with respect to teenagers in India, who are often heavy users and/or early adopters of new technologies.

The DPDP Act requires data fiduciaries to obtain verifiable consent<sup>148</sup> of the parent<sup>149</sup> of a child in the manner prescribed<sup>150</sup> before processing their personal

---

<sup>144</sup> Anil Padmanabhan, *Govt Amends Rules Pertaining to Maintaining of Books by Companies*, *Economic Times* (Aug. 10, 2022), <https://economictimes.indiatimes.com/news/economy/policy/govt-amends-rules-pertaining-to-maintaining-of-books-by-companies/articleshow/93623206.cms?from=mdr>.

<sup>145</sup> Indian Computer Emergency Response Team (CERT-In), *Directions Issued Under Section 70B of the Information Technology Act, 2000* (Apr. 28, 2022), [https://www.cert-in.org.in/PDF/CERT-In\\_Directions\\_70B\\_28.04.2022.pdf](https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf).

<sup>146</sup> Indian Computer Emergency Response Team (CERT-In), *FAQs on Cyber Security Directions*, [https://www.cert-in.org.in/PDF/FAQs\\_on\\_CyberSecurityDirections\\_May2022.pdf](https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf).

<sup>147</sup> Section 2(f) of the DPDP Act defines a 'child' to mean "an individual who has not completed the age of eighteen years."

<sup>148</sup> See Section 9(1) of the DPDP Act.

<sup>149</sup> Section 2(j) of the DPDP Act defines a 'Data Principal' to mean the individual to whom the personal data relates, and where such individual is a child, to include the parents of such child.

<sup>150</sup> See Rule 10 of the Draft Rules. Rule 11, read with the Fourth Schedule, of the Draft Rules provide exemptions from certain obligations applicable to the processing of a child's personal.

data. The Draft Rules require a data fiduciary to adopt appropriate technical and organizational measures to ensure that verifiable consent of the parent is obtained before the processing of any personal data of a child. The Draft Rules also require such data fiduciaries to “observe due diligence for checking that the individual identifying herself as the parent is an adult who is identifiable if required in connection with compliance with any law for the time being in force in India, by reference to— (a) reliable details of identity and age available with the Data Fiduciary; or (b) voluntarily provided details of identity and age or a virtual token mapped to the same, which is issued by an entity entrusted by law or the Central Government or a State Government with the maintenance of such details or a person appointed or permitted by such entity for such issuance, and includes such details or token verified and made available by a Digital Locker service provider.”<sup>151</sup>

Such requirements under the Draft Rules related to obtaining verifiable parental consent have caused some confusion among stakeholders.<sup>152</sup> In addition, the DPDP Act prohibits data fiduciaries from undertaking tracking, behavioural monitoring or targeted advertising in respect of children.<sup>153</sup> The DPDP Act also prohibits data fiduciaries from undertaking such personal data processing that is likely to cause any detrimental effect on the well-being of a child.<sup>154</sup> However, it is not clear what a ‘detrimental effect’ might be, and no separate guidance on ‘detriment’ has been provided in the DPDP Act.

The age threshold under the DPDP Act with respect to defining a child is high by global standards.<sup>155</sup> In the United States, for instance, the Children’s Online

---

<sup>151</sup> *Id.*

<sup>152</sup> See, e.g., <https://www.medianama.com/2025/01/223-data-protection-rules-2025-children-data-india/> and <https://www.hindustantimes.com/india-news/first-in-person-consultation-on-draft-dpdp-rules-101736881438001.html>.

<sup>153</sup> The Digital Personal Data Protection Act, No. 22 of 2023, § 9(3) (India).

<sup>154</sup> The Digital Personal Data Protection Act, No. 22 of 2023, § 9(2) (India).

<sup>155</sup> Pursuant to Article 8(1) of the GDPR, the default age at which the EU considers a person no longer to be a child – such that they can express valid consent under Article 6(1)(a) – is 16. Where the child is aged below 16, data processing will be lawful only if, and to the extent that, consent is provided or authorized by a holder of parental responsibility.

Privacy Protection Act (“**COPPA**”)<sup>156</sup> imposes certain requirements on operators of websites or online services directed at children, including social media platforms – but only in respect of children under 13 years of age. Since older teenagers are not explicitly covered by current US data protection laws, such teenagers are part of a marketplace whose business model combines data collection, profiling, tracking, and monitoring of social interactions. It is possible that such concerns led the MeitY to use a high threshold for defining children under the DPDP Act – although this may produce issues with respect to viability, access, compliance burdens, and monitoring concerns.

An important aspect of determining the appropriate age to define a child for the purpose of data protection laws includes considerations of feasibility. Other than protecting the privacy of children and safeguarding them from harm, laws need to be designed for implementation. While studies appear to indicate instances of non-compliance and/or undesirable outcomes in respect of both the COPPA<sup>157</sup> and the GDPR<sup>158</sup> in respect of processing children’s data, stipulating an upper age-limit as high as 18 while defining a child – as the DPDP Act does – might lead to abuse or workarounds, including by children and parents themselves. While it may be difficult to devise a fail-safe framework of verifying the identity of an under-18 person, the penalty for a breach in the observance of additional obligations in relation to children may extend up to INR 2 billion.<sup>159</sup>

## **10. Potential Relaxations**

The DPDP Act provides for the Government to declare by notification,

---

<sup>156</sup> Children’s Online Privacy Protection Rule (COPPA), Fed. Trade Comm’n, <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>.

<sup>157</sup> Irion, K., Helberger, N., & van Hoboken, J., *Won’t Somebody Think of the Children? Examining COPPA Compliance at Scale*, IMDEA Networks Institute (2018), [https://dspace.networks.imdea.org/bitstream/handle/20.500.12761/551/Wont\\_Somebody\\_Think\\_Children\\_Examining\\_COPPA\\_Compliance\\_Scale\\_2018\\_EN.pdf?sequence=1&isAllowed=y](https://dspace.networks.imdea.org/bitstream/handle/20.500.12761/551/Wont_Somebody_Think_Children_Examining_COPPA_Compliance_Scale_2018_EN.pdf?sequence=1&isAllowed=y).

<sup>158</sup> Sonia Livingstone & Monica Bulger, *A Global Research Agenda for Children’s Rights in the Digital Age*, 19 *New Media & Soc’y* 657 (2017), <https://journals.sagepub.com/doi/abs/10.1177/1461444816686327?journalCode=nmsa>.

<sup>159</sup> The Digital Personal Data Protection Act, No. 22 of 2023, § 33 & Schedule (India). .

before the expiry of five years from the date of commencement of the DPDP Act, that any provision of such Act will not apply to such data fiduciary or classes of data fiduciaries for a period as specified by such notification.<sup>160</sup> Accordingly, AI start-ups may be exempted from some obligations under the DPDP Act for a certain duration.

## **11. Consent Requirements and Challenges**

One of the most prominent features of the DPDP Act is its consent-centric approach,<sup>161</sup> requiring explicit permission from individuals before their PI can be processed.<sup>162</sup> Individuals may give, manage, review or withdraw their consent through a ‘consent manager’.<sup>163</sup>

AI developers will need to secure informed consents before using PI for training models. This can complicate the process of data collection, including in cases where extensive and/or curated datasets are required to function effectively (*e.g.*, generative AI systems). Investors in AI should assess the target company’s compliance with the SPDI Rules and the DPDP Act, including with respect to

---

<sup>160</sup> The Digital Personal Data Protection Act, No. 22 of 2023, § 17(5) (India).

<sup>161</sup> Digital Personal Data Protection Act, 2023, §§ 4(1)(a), 5, 6 (India); Draft Digital Personal Data Protection Rules, 2025, Rule 3(b), Ministry of Electronics & Information Technology, India (2025)

<sup>162</sup> Section 6(1) of the DPDP Act states: “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.” Also see Rule 3(b) of the Draft Rules.

<sup>163</sup> Section 2(g) of the DPDP Act defines a ‘Consent Manager’ to mean “a person registered with the Board, who acts 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 platform.” Section 6(7) of the DPDP Act states: “The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager.” Further, Rule 4, read with the First Schedule, of the Draft Rules, deals with the conditions for registration and the obligations of consent managers. For a discussion on the potential use of consent managers through India’s digital public infrastructure, see:

<https://www.snrlaw.in/indias-digital-public-infrastructure-could-have-all-the-answers-to-questions-under-the-dpdp-act/> and <https://www.thehindubusinessline.com/business-laws/indias-digital-public-infrastructure-could-have-all-the-answers-for-the-data-privacy-problem/article67448661.ece>. For a general discussion on managing consent under the DPDP Act.

potential liabilities for non-compliance. In addition, the use of data for AI development may be subject to sector-specific regulations, such as those governing the healthcare, financial, or telecommunications industries. The target company should have the necessary licenses, approvals, and consents to collect, store, process and use data in compliance with such laws and regulations.

Unlike the EU's GDPR, the DPDP Act does not recognize alternative legal bases for processing PI, such as contractual necessity<sup>164</sup> or legitimate interest.<sup>165</sup> This limitation could slow down the pace of AI development in India, especially across sectors that rely heavily on PI, potentially stifling innovation.

## **12. Data Minimization and Purpose Limitation**

The principles of 'data minimization' and 'purpose limitation'<sup>166</sup> imply that PI should be collected and used only as necessary, and for specified purposes alone.<sup>167</sup> This may restrict the ability of AI models to leverage large datasets for diverse applications and may lead to challenges in developing versatile AI systems capable of adapting to multiple use-cases.

## **13. Exemptions for Publicly Available Data**

---

<sup>164</sup> See Article 6(1)(b) of the GDPR: "Processing shall be lawful only if and to the extent that at least one of the following applies: ...processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."

<sup>165</sup> See Article 6(1)(f) of the GDPR: "Processing shall be lawful only if and to the extent that at least one of the following applies: ...processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

<sup>166</sup> Section 6(1) of the DPDP Act states: "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." Also see Sections 8(7) and 8(8) of the DPDP Act.

<sup>167</sup> For a discussion on data minimization, S&R Associates, *Navigating Data Minimization Requirements Under India's DPDP Act* (Apr. 2024), <https://www.snrlaw.in/navigating-data-minimization-requirements-under-indias-dpdp-act/>.

While the DPDP Act requires consent for most kinds of PI (barring certain legitimate uses),<sup>168</sup> it contains an exemption for publicly available data.<sup>169</sup> This exemption could facilitate AI training through the scraping of public information from social media platforms and other online sources.

However, on account of concerns regarding the potential misuse or breach of such data, AI organizations may need to ensure that the scraping of publicly available PI complies with other applicable laws and ethical standards.

Regulations such as the GDPR do not include specific exemptions for publicly available data and require organizations to adhere to strict guidelines regardless of how PI was obtained.<sup>170</sup> The DPDP Act does not impose an obligation on data fiduciaries to inform individuals about the use of their publicly available data. As a result, AI companies may be able to develop models in India more easily than in some other jurisdictions. However, in the event of misuse or overreach, legislative corrections and/or regulatory scrutiny may follow.

#### **14. Research Exemptions and Implications**

Organizations are allowed to process PI for research, archiving, or statistical purposes without adhering to certain obligations of the DPDP Act.<sup>171</sup> This exemption is contingent upon compliance with Government-set standards, which

---

<sup>168</sup> Digital Personal Data Protection Act, 2023, §§ 4(1)(b), 7 (India).

<sup>169</sup> Section 3(c)(ii) of the DPDP Act states: “Subject to the provisions of this Act, it shall...not apply to... personal data that is made or caused to be made publicly available by— (A) the Data Principal to whom such personal data relates; or (B) any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.”

<sup>170</sup> Seen Article 14 of the GDPR.

<sup>171</sup> Section 17(2)(b) of the DPDP Act states: “The provisions of this Act shall not apply in respect of the processing of personal data ... necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with such standards as may be prescribed.” Further, Rule 15 read with the Second Schedule of the Draft Rules prescribe the standards for such processing. Thus, Rule 15 (“Exemption from Act for research, archiving or statistical purposes”) of the Draft Rules state: “The provisions of the Act shall not apply to the processing of personal data necessary for research, archiving or statistical purposes if it is carried on in accordance with the standards specified in Second Schedule.”

are yet to be notified. However, such standards have been included in the Draft Rules.<sup>172</sup>

In contrast, regulations such as the GDPR permit research as a secondary use of PI<sup>173</sup> without requiring a distinct lawful basis for processing, provided appropriate safeguards are implemented to protect individual rights. Over time, technical and/or ethical standards may evolve in India to ensure that the DPDP Act's research-related exemption fosters responsible AI development. For instance, pursuant to a March 2018 taskforce report<sup>174</sup> and a discussion paper about India's national AI strategy,<sup>175</sup> NITI Aayog, under the Government had deliberated upon the advisability of regulating AI and proposed overarching principles for the development of 'responsible AI' pursuant to a February 2021 approach document.<sup>176</sup>

## **15. Compliance Burden and Legal Liabilities**

In general, the DPDP Act's compliance requirements are likely to increase operational costs for AI companies. AI companies may need to invest in robust governance frameworks to ensure adherence to consent management, data retention policies, and other obligations. Since non-compliance may result in substantial penalties, AI companies may prioritize compliance over innovation.

---

<sup>172</sup> Rule 15 read with the Second Schedule of the Draft Rules prescribe the standards for such processing. Thus, Rule 15 ("Exemption from Act for research, archiving or statistical purposes") of the Draft Rules state: "The provisions of the Act shall not apply to the processing of personal data necessary for research, archiving or statistical purposes if it is carried out in accordance with the standards specified in Second Schedule."

<sup>173</sup> Péter Kovács et al., *Artificial Intelligence and Its Challenges* (2018), <https://real.mtak.hu/106370/1/2052.2018.59.4.5.pdf>.

<sup>174</sup> Task Force on Artificial Intelligence, *Report of the Task Force on Artificial Intelligence* (Mar. 20, 2018), [https://psa.gov.in/CMS/web/sites/default/files/publication/Report\\_of\\_Task\\_Force\\_on\\_ArtificialIntelligence\\_20March2018\\_2.pdf](https://psa.gov.in/CMS/web/sites/default/files/publication/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf).

<sup>175</sup> NITI Aayog, *National Strategy for Artificial Intelligence: Discussion Paper* (Jan. 2019) <https://www.niti.gov.in/sites/default/files/2019-01/NationalStrategy-for-AI-Discussion-Paper.pdf>.

<sup>176</sup> NITI Aayog, *Responsible AI: National Strategy for Artificial Intelligence* (Feb. 22, 2021), <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf>.

## **16. Ethical Considerations and Bias Mitigation**

With increased scrutiny on data use, policy considerations surrounding bias in AI models are likely to become more prominent. The final rules issued under the DPDP Act are likely to compel organizations, and especially SDFs, to address potential biases and ensure fairness in their algorithms,<sup>177</sup> including through DPIAs and data audits.<sup>178</sup> Such requirements may demand additional resources and methodologies during the development phase.

## **17. Potential Role of AI in Compliance Management**

AI technologies themselves may be able to assist in managing compliance with the DPDP Act. For example, AI could assist with data mapping.<sup>179</sup>

## **18. Limited Territorial Scope and Consequences**

Since the DPDP Act applies extraterritorially only when data processing is connected to offering goods or services to individuals in India,<sup>180</sup> offshore providers of AI systems which do not directly offer goods or services within India may be able to process PI of Indian citizens without any restrictions.

This limitation contrasts with broader frameworks like the GDPR, which

---

<sup>177</sup> Rule 12(3) of the Draft Rules states: “A Significant Data Fiduciary shall observe due diligence to verify that algorithmic software deployed by it for hosting, display, uploading, modification, publishing, transmission, storage, updating or sharing of personal data processed by it are not likely to pose a risk to the rights of Data Principals.”

<sup>178</sup> Rule 12(2) of the Draft Rules states: “A Significant Data Fiduciary shall cause the person carrying out the Data Protection Impact Assessment and audit to furnish to the Board a report containing significant observations in the Data Protection Impact Assessment and audit.”

<sup>179</sup> For a discussion on data mapping, S&R Associates, *It’s Personal: A Roadmap for Data Mapping in Digital India* (2024), <https://www.snrlaw.in/its-personal-a-roadmap-for-data-mapping-in-digital-india/>.

<sup>180</sup> See Section 3(b) of the DPDP Act. Also see Rule 14 of the Draft Rules related to processing of personal data outside India: “Transfer to any country or territory outside India of personal data processed by a Data Fiduciary...outside the territory of India in connection with any activity related to offering of goods or services to Data Principals within the territory of India, is subject to the restriction that the Data Fiduciary shall meet such requirements as the Central Government may, by general or special order, specify in respect of making such personal data available to any foreign State, or to any person or entity under the control of or any agency of such a State.”

applies extraterritorially not only based on goods/service offerings, but also in terms of monitoring the behaviour of individuals within the EU's jurisdiction. Foreign entities may be able to take advantage of the limited extraterritorial scope of the DPDP Act by profiling Indian citizens without consent. Relative to a previous draft bill,<sup>181</sup> individual 'profiling' has been excluded from the scope of extraterritorial application under the DPDP Act.<sup>182</sup> Thus, 'Big Data' analytics for evaluative and targeting purposes can continue. Further, the use of third-party cookies – including those used by data brokers, analytics firms and 'ad-tech' platforms may also be permitted, especially if the processing is done extraterritorially. This may be particularly relevant for technology companies, including social media platforms and website aggregators, which have 'persistent identifiers' to track consumer behaviour.

### **19. Consent Withdrawal and Data Erasure**

The DPDP Act provides data principals with an option to withdraw their consent<sup>183</sup> and requires data fiduciaries to *not* retain PI once the purpose of processing has been accomplished.<sup>184</sup> When consent is withdrawn by an individual, a data fiduciary must also ensure that the processing stops within a reasonable period,<sup>185</sup> followed by data erasure.<sup>186</sup> Further, data principals may ask for their data to be erased, corrected, completed, or updated.<sup>187</sup>

In this regard, AI companies may find it challenging to purge or amend PI from their systems. Among potential options to address these requirements,

---

<sup>181</sup> Ministry of Electronics & Information Technology, Government of India, *The Digital Personal Data Protection Bill, 2022*,

[https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022\\_0.pdf](https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022_0.pdf).

<sup>182</sup> For a summary of the differences between the previous draft bill and the DPDP Act.

<sup>183</sup> Digital Personal Data Protection Act, 2023, § 6(4) (India).

<sup>184</sup> Digital Personal Data Protection Act, 2023, §§ 6(6), 8(7) (India).

<sup>185</sup> Digital Personal Data Protection Act, 2023, § 6(6) (India)..

<sup>186</sup> Digital Personal Data Protection Act, 2023, § 8(7) (India).

<sup>187</sup> Digital Personal Data Protection Act, 2023, § 12(1) (India)..

‘Machine Unlearning’ (“**MU**”) techniques could prove useful,<sup>188</sup> including for large and cost-intensive models that are difficult to re-train. The goal of MU is to create an unlearned model which behaves similar to a model re-trained on the same data minus the information that needs to be forgotten/changed.

## VII. REGULATORY DEVELOPMENTS ON NON-PERSONAL DATA

According to a December 2017 white paper released by a government-constituted expert committee (the “**Expert Committee**”), data which is viewed as non-personal information can be combined with other datasets to create personally identifiable information, including via de-anonymization techniques. Accordingly, the Expert Committee suggested that it is possible for personal or non-personal data, when processed using ‘big data’ analytics, to be transformed into SPDI.

In addition, the Expert Committee took note of research studies that acknowledge the difficulties of distinguishing between personal and non-personal data.<sup>189</sup>

### A. THE JOINT COMMITTEE REPORT

A December 2021 Joint Committee report (the “**JC Report**”) presented in Parliament also observed that it was impossible to clearly distinguish between personal and non-personal data. Accordingly, the JC Report recommended that both categories of data should be included within the same statute.

### B. DATA GOVERNANCE COMMITTEE AND ITS REPORTS

In September 2019, the MeitY constituted a committee of experts (“**DG Committee**”) to (i) deliberate on a data governance framework, and (ii) examine

---

<sup>188</sup> Subcommittee on Artificial Intelligence, *Report on AI Policy and Regulatory Framework* (Dec. 26, 2023) <https://indiaai.s3.ap-south-1.amazonaws.com/docs/subcommittee-report-dec26.pdf>.

<sup>189</sup> For a discussion on the distinction between personal and non-personal data, S&R Associates, *Personal and Non-Personal Data in Digital India: Before and After*, S&R Law (Sept. 18, 2023), <https://www.snrlaw.in/personal-and-non-personal-data-in-digital-india-before-and-after/>

issues related to regulating non-personal data.

### **1. First Report**

A draft version of the DG Committee's first report, released in July 2020 ("**First DGC Report**"),<sup>190</sup> provided a definition of non-personal data and divided such data into three categories involving public, community, and private perspectives, respectively. Further, the First DGC Report defined key roles with regard to non-personal data (such as data principal, data custodian, and data trustee) and an institutional form of data infrastructure (data trust). It also defined a 'data business' in light of the proliferation of big data analytics and AI – which, in turn, had led to the creation of information-intensive services and value in the global data economy.

Thus, a 'data business' was envisaged as one that collects, processes, stores, or otherwise manages information, and meets certain criteria. Accordingly, businesses which collect data beyond a critical threshold may get categorized as a data business in the future.

In addition, the First DGC Report recommended mechanisms for data sharing. In that regard, it proposed a separate legislation to govern and regulate non-personal data, including through technology-related guidelines for digitally implementing recommended rules around data sharing.

### **2. Revised Report**

Pursuant to stakeholder feedback, the DG Committee proposed a revised version of the First DGC Report ("**Revised DGC Report**").<sup>191</sup> In the Revised

---

<sup>190</sup> Ministry of Electronics & Information Technology, Government of India, *Report by the Committee of Experts on Non-Personal Data Governance Framework* (July 2020), <https://ourgovdotin.wordpress.com/wp-content/uploads/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf>.

<sup>191</sup> Ministry of Electronics & Information Technology, Government of India, *Revised Report by the Committee of Experts on Non-Personal Data Governance Framework* (Dec. 2020), <https://ourgovdotin.wordpress.com/wp-content/uploads/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf>.

DGC Report, the DG Committee expanded on the idea of high-value datasets, along with a data trustee that manages such datasets. It also differentiated the roles of a data custodian and a data processor, respectively.

Furthermore, the DG Committee recognized existing practices among private organizations with respect to sharing data for the purpose of boosting profits. Accordingly, the Revised DGC Report made no recommendations with respect to business-related data sharing. However, it retained key features of the First DGC Report, including those related to consent requirements for anonymized data and data businesses.<sup>192</sup>

### C. DRAFT NATIONAL DATA GOVERNANCE FRAMEWORK POLICY

In May 2022, the MeitY released a draft of the ‘National Data Governance Framework Policy’ (“**Draft NDGFP**”).<sup>193</sup> Among other things, the Draft NDGFP aims to ensure that non-personal and anonymized data from both government and private entities are accessible by research and innovation ecosystems, including for the purpose of facilitating data and AI-based R&D initiatives by Indian start-ups.<sup>194</sup> The draft policy also aims to promote transparency, accountability, and ownership with respect to dataset access.<sup>195</sup> In that regard, the Draft NDGFP called for the creation of the IDP and seeks to provide an institutional framework for the sharing of such non-personal datasets while ensuring privacy, security, and

---

<sup>192</sup> For an overview of the regulatory trajectory of India’s digital governance framework, S&R Associates, *India’s Proposed Digital Governance Framework: Past Developments and Present Status*, S&R Law (Apr. 4, 2023), <https://www.snrlaw.in/indias-proposed-digital-governance-framework-past-developments-and-present-status/>.

<sup>193</sup> Ministry of Electronics & Information Technology, Government of India, *National Data Governance Framework Policy* (June 2022), <https://www.meity.gov.in/writereaddata/files/National-Data-Governance-Framework-Policy.pdf>.

<sup>194</sup> Press Information Bureau, *Cabinet Approves National Data Governance Framework Policy*, PIB (June 7, 2023) <https://pib.gov.in/PressReleasePage.aspx?PRID=1845318>.

<sup>195</sup> *Draft National Data Governance Framework Policy*, The Hindu Centre for Politics and Public Policy (May 2022), <https://www.thehinducentre.com/resources/national-data-governance-framework-policy-draft-may-2022-pdf-50821-kb/article67556983.ece#:~:text=The%20Ministry%20of%20Electronics%20andpersonal%20data%20and%20datasets%20access.>

trust.

## **D. IDP**

Since the application of advanced analytics and AI to non-personal data can lead to economically beneficial outcomes,<sup>196</sup> and consistent with the Draft NDGFP, the IDP was included as one of the main pillars of India's AI mission to harness the benefits of AI.<sup>197</sup> The IDP aims to facilitate access to non-personal data and high-quality AI-ready datasets for the purpose of empowering Indian startups and researchers.<sup>198</sup>

In February 2023, while presenting the Union Budget, India's Finance Minister had indicated that the NDGFP might be finalized soon, enabling access to anonymized data (see [here](#) and [here](#)). Although reports from 2024 suggest that a revised final version of the Draft NDGFP has been prepared by the Government, an official copy is yet to be released.

## **VIII. DIGITAL INDIA ACT**

While the DPDP Act is poised to replace the Existing Regime, it seeks to omit or amend only certain sections of the IT Act (such as Section 43A). However, the proposed Digital India Act<sup>199</sup> is expected to repeal the IT Act<sup>200</sup> in its entirety,

---

<sup>196</sup> Rahul Matthan, *Data Marketplaces: The Next Frontier*, The Hindu (Feb. 28, 2024), <https://www.thehindu.com/opinion/op-ed/data-marketplaces-the-next-frontier/article67972022.ece>.

<sup>197</sup> Press Information Bureau, *Union Cabinet Approves India AI Mission*, PIB (Mar. 7, 2024), <https://pib.gov.in/PressReleasePage.aspx?PRID=2012375>.

<sup>198</sup> For more details on the IDP and India's AI Mission, S&R Associates, *India's Initiatives on Regulating Artificial Intelligence: Balancing Promotion with Protection*, S&R Law (Jan. 18, 2024), <https://www.snrlaw.in/indias-initiatives-on-regulating-artificial-intelligence-balancing-promotion-with-protection/> and S&R Associates, *Investing in AI in India (Part 2): Tracking the Regulatory Landscape*, S&R Law (Jan. 31, 2024), <https://www.snrlaw.in/investing-in-ai-in-india-part-2-tracking-the-regulatory-landscape/>.

<sup>199</sup> Ministry of Electronics & Information Technology, Government of India, *Digital India Act – Presentation for Stakeholder Consultation* (Mar. 9, 2023), [https://www.meity.gov.in/writereaddata/files/DIA\\_Presentation%2009.03.2023%20Final.pdf](https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf).

<sup>200</sup> Press Information Bureau, *Consultations Begin on the Digital India Act, 2023*, PIB (Mar. 10, 2023), <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1948357>.

along with the rules framed under it (barring the SPDI Rules), including the Intermediary Guidelines.

According to media reports from February<sup>201</sup> and March<sup>202</sup> 2023, the Government may frame rules for sharing anonymized personal data and non-personal data under the Digital India Act – such as in respect of data captured by invasive gadgets.<sup>203</sup>

## IX. THE WAY AHEAD

India's evolving data protection regime, in terms of both personal and non-personal information, constitutes areas of concern as well as opportunity for AI developers, deployers, and investors. Accordingly, such stakeholders need to exercise caution, set up a plan, and prepare for the way ahead, including by keeping track of regulatory and other developments with regard to ongoing compliance and growth.

Relevant entities should first acquire a proper understanding of legal requirements – some of which can vary depending on (i) a company's role in the AI value chain, as well as (ii) the risk profile of an AI system. The main preparatory steps could include the following:

- establishing a cross-functional team;

---

<sup>201</sup> Hindustan Times, *Govt May Frame Rules for the Sharing of Non-Personal Data Under Digital India Law*, Hindustan Times (Mar. 3, 2023), <https://www.hindustantimes.com/india-news/govt-may-frame-rules-for-the-sharing-of-non-personal-data-under-digital-india-law-101677355138634.html>.

<sup>202</sup> Medianama, *30 Talking Points from the Digital India Act Consultation*, Medianama (Mar. 15, 2023) <https://www.medianama.com/2023/03/223-30-talking-points-digital-india-act-consultation/>.

<sup>203</sup> Hindustan Times, *Rules for Invasive Gadgets Likely Under Digital India Act: MoS Chandrasekhar*, Hindustan Times (Mar. 13, 2023), <https://www.hindustantimes.com/technology/rules-for-invasive-gadgets-likely-under-digital-india-act-mos-chandrasekhar-101678376174708.html>. For a discussion on the broad themes likely to be included in the Digital India Act, S&R Associates, *Back to the Future: India's Proposed Digital Governance Framework*, S&R Law (Mar. 2023), <https://www.snrlaw.in/back-to-the-future-indias-proposed-digital-governance-framework/>.

- engaging expert resources;
- performing a comprehensive assessment of the scope and risk profile of current and planned AI systems;
- developing a compliance plan and related policies;
- establishing governance mechanisms and program management;
- establishing reporting and oversight procedures;
- maintaining comprehensive records and documentation;
- performing ongoing monitoring; and
- reviewing and updating cybersecurity measures.<sup>204</sup>

Companies may be able to leverage certain aspects of their data protection compliance programs to comply with requirements under India's regulatory regime on AI, including in respect of data governance. For instance, policies and processes for managing personal data under the DPDP Act could provide a foundation for responsible data use and oversight while developing or deploying AI systems. Further, built-in checks and controls, including those related to cybersecurity and data breaches, could minimize the risks involved, especially in respect of handling personal information.

In addition, companies could adapt their future approaches and methodologies on privacy and data protection impact assessments for the purpose of evaluating AI-related risks, including in respect of use cases, training data, as well as impacts on individual rights. Regular reviews of information systems under the DPDP Act, such as data and process mapping, may provide clarity about how information moves into and across an organization – thus highlighting both risks and unknown factors.

Further, maintaining records of data processing activities could provide

---

<sup>204</sup> In the context of the European Union's Artificial Intelligence Act and the General Data Protection Regulation (GDPR): <https://www.snrlaw.in/the-eus-new-law-on-artificial-intelligence-global-implications/>.

valuable documentation and audit trails to demonstrate key measures taken by an entity in respect of AI governance. Such records may also prove useful to ensure that rights related to IP are appropriately addressed.

In the short term, potential impacts might include increased compliance costs along with delays in the development and deployment of AI systems, which may, in turn, reduce the pace of innovation in AI technology. However, in the medium and long term, proper planning may produce several benefits, such as by (1) changing the way in which AI systems are developed, tested, documented and deployed, with an increased focus on trustworthy and responsible AI,<sup>205</sup> as well as (2) drawing more investment on AI safety. Further, harmonized AI safety standards could stimulate the emergence of a new global framework.

Given that the DPDP Act is likely to come into force soon, AI systems that process personal data in ways that contravene the DPDP Act's principles of purpose limitation and data minimization could attract significant penalties. Developers must therefore ensure that, to the extent possible, personal data is either anonymized or used with explicit consent where AI model training is concerned. Further, they should incorporate robust internal compliance mechanisms and implement appropriate technical and organizational measures to align their operations, models, and practices with the DPDP Act's requirements.

The proposed Digital India Act is also likely to shape how AI models are

---

<sup>205</sup> See, e.g., <https://www.investindia.gov.in/blogs/ensuring-responsible-and-trustworthy-ai-all#:~:text=It%20aimed%20to%20establish%20broad,Principle%20of%20Safety%20and%20Reliability>. In this regard, NITI Aayog, the Government's policy thinktank, along with other agencies have issued guidelines and recommendations with respect to responsible AI development and deployment. For instance, see NITI Aayog's 'Approach Document for India' dated February 2021, which formulated certain principles for responsible AI, available at: <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf>. Also see 'THE DEVELOPER'S PLAYBOOK for Responsible AI in India,' released by NASSCOM in collaboration with the MeitY and others in November 2024, available at: <https://nasscom.in/ai/pdf/the-developer-s-playbook-for-responsible-ai-in-india.pdf>. For a Government update dated October 2024 on India's evolving commitment to build safe and trusted AI, including by supporting new research projects on critical themes such as MU, synthetic data generation, bias mitigation, ethical AI frameworks, privacy-enhancing strategies, explainable AI, AI governance testing, and algorithmic auditing tools, see: <https://pib.gov.in/PressReleasePage.aspx?PRID=2065579>.

developed and deployed in India, including by imposing stringent requirements around consent, data use, and ethical considerations with respect to non-personal information. Balancing compliance with innovation will remain crucial for organizations as they aim to thrive under India's emerging legal and regulatory frameworks on data and AI, respectively.

The path forward demands a delicate balance, akin to a high-wire act performed on the global stage. It calls for regulators to become not just enforcers, but visionaries; for market participants to embrace not just profit, but responsibility; and for technologists to consider not just what can be done, but what should be done. This harmonization of interests is not merely aspirational – it is essential for the continued vitality and integrity of our financial markets.