COMMENTS SUBMITTED
ON
THE 'REPORT ON AI GOVERNANCE GUIDELINES DEVELOPMENT'

TO THE
**MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY (MEITY),
GOVERNMENT OF INDIA**

BY
DHIRUBHAI AMBANI UNIVERSITY – SCHOOL OF LAW
GANDHINAGAR, GUJARAT, INDIA
&
REGHORIZON, SWITZERLAND

BY

PROF. (DR.) AVINASH DADHICH
FOUNDING DIRECTOR,
DHIRUBHAI AMBANI UNIVERSITY - SCHOOL OF LAW

AYISHA PIOTTI,
MANAGING PARTNER,
REGHORIZON, SWITZERLAND

DR. SHOUVIK KUMAR GUHA
NON-RESIDENT FELLOW,
DHIRUBHAI AMBANI UNIVERSITY - SCHOOL OF LAW

AATMAN SHUKLA
ASSISTANT PROFESSOR,
DHIRUBHAI AMBANI UNIVERSITY - SCHOOL OF LAW

AUTHOR PROFILES

Ayisha Piotti

MANAGING PARTNER, REGHORIZON, SWITZERLAND

Ayisha Piotti is the head of the AI Policy Summit, an annual event jointly organized by the ETH Zurich Center for Law & Economics and RegHorizon. Ayisha has over 20 years of experience in the private & public sector, including with the United Nations. Prior to joining ETH Zurich, Ayisha created the Swiss based strategic consulting firm RegHorizon and was Senior Director of Business Development and Corporate Affairs within a large multinational, where she built and led cross-functional teams and projects spanning diverse geographies, including Europe, Middle East, Africa and Asia. She is also actively engaged in various organisations promoting women in leadership and technology.

Dr. Shouvik Kumar Guha

NON-RESIDENT FELLOW, DHIRUBHAI AMBANI UNIVERSITY - SCHOOL OF LAW

Dr. Shouvik Kumar Guha is a Non-Resident Fellow at the Dhirubhai Ambani University – School of Law (DA-SoL) and an Associate Professor at the West Bengal National University of Juridical Sciences (WBNUJS) Kolkata has a thorough understanding in the areas of Mergers & Acquisitions (M&A), Intellectual Property and competition law. Dr. Guha's academic contributions and professional experience have made him a distinguished figure in Indian legal academia. His specialization in Technology Transfer, IP and Antitrust laws makes him an expert in interpreting complex legal frameworks in these areas.

Prof. (Dr.) Avinash Dadhich

FOUNDING DIRECTOR, DHIRUBHAI AMBANI UNIVERSITY - SCHOOL OF LAW

Prof. (Dr.) Avinash Dadhich is the founding director of the Dhirubhai Ambani University – School of Law (DA-SoL), and also serves as a Global Advisory Board Member for AMS Ethical AI, where his expertise in AI ethics is vital in guiding responsible integration of artificial intelligence in talent acquisition. In his academic career, he has held senior roles, including Director at Manipal Law School, MAHE, Bengaluru, and Dean at IFIM Law School, Bengaluru. He was invited as a visiting research fellow at the Max Planck Institute of IP and Competition, Munich; the Institute of European Studies, Brussels; and at King's College London.

Asst. Prof. Aatman Shukla

ASSISTANT PROFESSOR, DHIRUBHAI AMBANI UNIVERSITY - SCHOOL OF LAW

With an LL.M. from the University of California, Berkeley, with a focus on Intellectual Property and Technology Law, Assistant Prof. Aatman Shukla seeks to bring a unique perspective to legal education, blending international legal education with practical Indian law experience to foster a multifaceted, dynamic legal approach. Having completed his BA.LLB (Hons.) from National Law University Delhi, his areas of expertise also include Contracts Law, Risk Mitigation and he has authored and co-authored numerous publications, bringing to the table significant academic and practical experience in his young career.

Contents

EXECUTIVE SUMMARY

The comments submitted by Dhirubhai Ambani University (DAU) – School of Law, India, and RegHorizon, Switzerland, critically assess the Ministry of Electronics & Information Technology (MeitY), Government of India's 'Report on AI Governance Guidelines Development' or 'the Report'. These comments highlight key areas of concern and propose recommendations to ensure the development of an inclusive and effective AI governance framework.

Concerns raised include the adoption of AI governance standards established by the Global North, failing to recognize the distinct and more pressing needs of the Global South. Given AI's potential for supercharging efficiency and governance, India should develop AI governance principles tailored to its socio-economic realities. Further, the Report has noble intentions of adhering to a baseline framework of AI Ethics and Regulations, but a one-size-fits-all approach runs the risk of both, overregulation and under-regulation for AI applications.

The Report also addresses copyright concerns in training AI models, but fails to shed light on fair-dealings policies. Also, the proposal to establish a Technical Secretariat under MeitY's supervision raises concerns about regulatory capture, which might result in government or Big Tech AI projects receiving preferential treatment, or evolving in a manner unsuited and antithetical to the public good. To maintain independence, an oversight body with representatives from academia, industry, and civil society should be considered.

In conclusion, DAU and RegHorizon emphasize the need for a nuanced and risk-based AI governance framework. Key recommendations include developing AI governance principles suited to the Global South, adopting a risk classification system, establishing clear copyright policies, preventing regulatory capture, ensuring diverse representation in AI governance bodies, and maintaining flexibility in transparency requirements. Implementing these recommendations will help India create an AI governance framework that fosters innovation while protecting fundamental rights, privacy, and accountability.

1. Opportunity to Form AI-governance principles for the Global South.

The Report on AI Governance Guidelines Development (henceforth, 'the Report') places great reliance on standards and principles developed by nations from the Global North, despite the difference in priority that AI and its applications may enjoy in such nations compared to those from the Global South. For the latter, use of AI-based solutions to solve governance and accessibility concerns may be more of an urgency, which is why the risk-reward equations will differ. By only recognizing and incorporating pre-existing ethical principles and standards, reflecting the values of the over-represented Global North[1] into national AI policy, India runs the risk of shunting aside key perspectives from marginalized or underrepresented communities. This ultimately runs contrary to the purpose for which it intends to use AI, i.e. in order to serve as a tool for capacity-building, unlocking the untapped potential of countries which have traditionally provided a cheap labour and workforce to the Global North, thus bridging the material and commercial gap between the Global North and Global South.[2]

Recommendation: Instead of merely reflecting the ethical principles baked into AI algorithms already, the Report should instead serve as a foundational stepping stone to initiate timely conversations about the need to curate and pioneer our very own AI-governance principles for the Global South.

2. Lack of Distinction between Buyer-to-Buyer (B2B) & Buyer-to-Customer (B2C) AI applications.

"*Since 2016, several organisations from government, industry, and civil society have published "principles" for "responsible and trustworthy AI (RTAI)". These set out a vision for the development, deployment, and use of AI systems that should inform the design of*

[1] Catherine Roche, P.J. Wall & David Lewis, *Ethics and Diversity in Artificial Intelligence Policies, Strategies and Initiatives*, 3 AI ETHICS 1095 (2023), https://doi.org/10.1007/s43681-022-00218-9.
[2] Horlane Mbayo, *Data and Power: AI and Development in the Global South*, OXFORD INSIGHTS (Oct. 2020), available at https://oxfordinsights.com/insights/data-and-power-ai-and-development-in-the-global-south/.

regulation of such systems as well. Much work has also already been done in India to put principles of AI governance into practice. In India, the principles from the apex government think tank and NASSCOM represent a good baseline from government and industry, respectively."

- Page 3, Report on AI Governance Guidelines Development

The Report refers to a series of governance principles and possible implementation avenues for those. In doing so, it appears to have made no difference between AI-applications that involve businesses at both the ends of their usage (B2B AI applications), as compared to those applications that involve consumers as well as businesses (B2C AI applications). It is likely that the nature of concerns including but not limited to data protection, privacy and harm potential will differ between such two categories, a factor that the Report falls short of addressing.

To elaborate, B2C AI applications should involve the processing of significant amounts of personal data of individual users, [3] which would bring them within the purview of data privacy legislations such as the General Data Protection Regulation (GDPR) in Europe, the California Consumer Protection Act or the Digital Personal Data Protection Act (hereafter, the DPDP Act), in India. Such applications would bring along with them significant imputations regarding individual autonomy of users, transparency in decision-making and discriminatory biases in training datasets.[4] The high-risk of harm caused by such applications would require incorporation of strong consent mechanisms, explainability requirements[5] and laying down a framework for redressal if these B2C AI applications are to live up to the fairness and transparency standards, along with no-harm principles that the Report envisions.[6]

[3] *DPDP Act*, §2(t) (2023).

[4] Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995 (2016).

[5] Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017).

[6] Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU AI Act*, 22 COMPUT. L. REV. INT'L 97 (2021).

In contrast, most B2B AI applications should not involve processing of personal data of individuals on a day-to-day basis.[7] Rather they would be used to process structured company data, and if it involves any personal data, the person would have notice of the same under the provisions of the DPDP Act imposing duties upon data fiduciaries.[8] Here, liability concerns would be less about the rights of individual users, and more about processing of information indicative of trade secrets or offering a competitive advantage to the companies in question, and allocation of liability would be decided by contractual obligations, rather than imposed by privacy legislations which typically come into play in cases of direct harm to individual users.

Recommendation: We recommend differentiating regulatory frameworks for B2B and B2C AI applications, recognizing their unique risks.

1. **B2C AI Applications**: These applications process significant personal data, requiring compliance with data privacy regulations like the DPDP Act and GDPR. Implement strong consent mechanisms, ensure AI explainability, and establish a grievance redressal framework for consumers.
2. **B2B AI Applications**: These applications typically process company data, with liability concerns focused on trade secrets and fair competition rather than individual privacy. Liability should be governed by contractual agreements between businesses, with limited privacy regulation focused on corporate data.
3. **Clear Guidelines**: The Reprt should clearly distinguish between B2B and B2C AI governance, ensuring tailored standards, oversight, and enforcement.

This differentiated approach will promote fairness, transparency, and accountability in AI systems, addressing the specific risks associated with each category.

[7] Zarsky *supra* note 4.
[8] *DPDP Act*, §4 (2023).

3. NEED FOR TIERED RISK-CLASSIFICATION OF AI APPLICATIONS TO ENSURE THERE IS NO ONE-SIZE-FITS-ALL APPROACH, AS IT MAY BE INHIBITING INNOVATION.

> "*The risks posed by a system depends not just on their capability, but on the context of deployment as well. The categorisations of systems purely based on computational capacity or data parameters may not be effective. For systems deployed in tightly regulated sectors, they would need to be assessed under existing sectoral laws before we evaluate the need for additional or fresh laws. The testing of such sectoral laws should, in particular, examine how existing rules on assigning liability for non-compliances (e.g., in health, banking, financial services and insurance, energy, etc.) can be applied to AI systems prone to high-risk. However, there may well be situations where a sectoral view is limiting, since we may not fully understand (i) the risks and/or (ii) the possibility for risks to spillover across sectors. Therefore, a view that "high risk scenarios" are likely only in tightly regulated sectors may not be correct. Given this, as well as the fact that many governance concerns may be common or cross-cutting across sectors, it might be useful to start examining a baseline framework to ensure transparency and responsibility across the overall AI ecosystem*"
>
> -Page 12, Report on AI Governance Guidelines Development

The lack of distinction between B2B AI applications & B2C AI applications brings us directly to another lacuna in the Report, which is the absence of clear definitions and classifications of risk as posed by different kinds & use-cases of AI applications. For instance, the EU AI Act categorizes AI into 4 categories based on their risk-level, namely minimal, limited, high, and unacceptable risk.[9] The EU AI Act envisions that high-risk applications, such as those used in critical infrastructure, biometrics, education, healthcare, workplace management and finance, must comply with strict transparency, data governance, and human oversight requirements.[10] However, the EU AI Act does not have onerous compliances for AI applications that are deemed minimal or no risk, such as chatbots, AI spam filters, AI recommendations, spell-checkers etc. which do not carry any

[9] *Regulation (EU) 2024/1689*, art. 5; *Regulation (EU) 2024/1689*, art. 6.

[10] *Regulation (EU) 2024/1689*, art. 6; *Regulation (EU) 2024/1689*, Annex III: High-Risk AI Systems Referred to in Article 6(2).

requirements for extensive oversight or prior approval, apart from requiring disclosure that the user is interacting with an AI, or content labelling obligations in case of generative AI. While the OECD AI Principles which are referred to in the Report do not have a risk-tiering approach, they do recommend sector-specific risk classifications based on factors such as data sensitivity, user impact, and potential for societal harm.[11]

As the Report does not define a low-risk or medium-risk category, it implies that all AI applications might be subject to blanket AI principles without differentiation. While this provides greater clarity, and ensures that there is an across-the-board applicability of principles to AI stakeholders, it also acts as a deterrent to the potential for further innovation in low-risk AI applications as they are restrained by the same prohibitions that are applicable on high-risk AI applications.

Recommendation: Without a tiered risk framework, AI applications become subject to one-size-fits-all regulations, which could either be too lenient for high-risk AI (e.g., biometric surveillance) or too strict for low-risk AI (e.g., chatbots, recommendation engines). This seems to be an oversight as the Report even envisages the starting-point of regulation as "*"activity-based regulation" through which people are motivated to minimise the risk of harms*", which implies that there should also be a proportionality in regulatory obligations, meaning high-risk AI should face stricter requirements while low-risk AI should be less stringently regulated.

The lack of a tiered classification of AI applications also has a further downstream effect, as it precludes India from aligning itself with a best practice of instituting sandboxes for low-risk and medium-risk AI applications which could be tested before introduction into the common market.[12] This would encourage, rather than inhibit, innovation in AI development as there would be room for AI companies to stress-test their technologies in a controlled environment, receive feedback about the same and work out kinks and

[11] Clark J., Murdick D., Perset K., & Grobelnik M., *The OECD Framework for Classifying AI Systems to Assess Policy Challenges and Ensure International Standards in AI*, OECD.AI, https://oecd.ai/en/wonk/classification.
[12] Buocz, T., Pfotenhauer, S., & Eisenberger, I., *Regulatory Sandboxes in the AI Act: Reconciling Innovation and Safety?*, 15 LAW, INNOVATION & TECH. 357, 357–89 (2023), https://doi.org/10.1080/17579961.2023.2245678.

roadblocks that typically feature in initial iterations of a product, to produce a better, more market-suited and consumer-centric final product.[13]

4. OVER-EMPHASIS ON TECHNO-REGULATORY MODEL.

> "*Given this, a conventional "command-and-control" governance strategy may not be able to adequately monitor, oversee or promote the growth and expansion of this space. There is value in integrating a "techno-legal" approach into the governance strategy, where legal and regulatory regimes are supplemented with appropriate technology layers (e.g., of governance technology tools along with adequate human oversight) across actors and systems.......................................There can be several different components to make up such a strategy. As a starting point, there is merit in examining how technology artefacts, similar to the concept of "consent artefacts" already proposed by MeitY in their Electronic Consent Framework, can perhaps leveraged to assign immutable and unique identities to participants, so that their activities can be tracked and recorded to establish liability chains between them Such artefacts, combined with the contracts between the participants, may allow for liability to be spread and distributed between them. Such a chain could allow for each member of the chain to enforce or require good behaviour on their own part and the part of the chain they are connected to such as their suppliers. This could potentially enable successful self-regulation across the ecosystem.*"
>
> - Page 6, Report on AI Governance Guidelines Development

The Report highlights and encourages the use of technology artefacts to get the participants across the entire value-chain of AI-usage to be assigned immutable and unique identities, with the intention of establishing liability chains and self-regulation standards. It seems to favour this approach compared to the so-called 'command and control' approach. Undoubtedly, adopting the latter would not have been a wise call; however, the solitary use-case example that the Report cites in this regard is the use of 'consent artefacts' that MeITy itself had proposed earlier -this appears to be divorced from the ground reality to a certain extent, since the consent artefacts had never been designed to facilitate assignment

[13] *Ibid.*

of such identities for all the players within the chain, such as consent managers from example.

Recommendation: A forcible attempt to use a techno-regulatory model by attempting to utilize consent-artefact analogues in an uncharted environment may have adverse implications for the entire data privacy and data security ecosystem that India currently has in place. A more coordinated and cautious approach grounded in reality, keeping in consideration the DPDP Act and associated Rules may be merited here.

5. COPYRIGHT CONCERNS AND AMBIGUITY AS TO WHETHER DATA SCRAPING FOR TRAINING AI MODELS CONSTITUTES FAIR DEALINGS

"*Given that copyright law grants the copyright holder an exclusive right to store, copy etc., creation of datasets using copyrighted works for training foundation models, without the approval of the right holder, can lead to infringement. The Indian law permits a very closed list of activities in using copyrighted data without permission that do not constitute an infringement. Accordingly, it is clear that the scope of the exception under Section 52(1)(a)(i) of the Copyright Act, 1957 is extremely narrow…………………..There are also policy level questions – for example, should AI systems be allowed to train on bulk datasets that may include copyrighted data, without taking approval from each copyright holder? If so, under what circumstances this may be considered so that rights of the copyright holders are not infringed? Do we need to interpret or clarify the scope of rights that should exist with the copyright holder? What guardrails must be introduced, if we are able to address the questions above? The answers can help improve legal certainty and clarify the way forward for a lawful use of AI systems.*"

-Pages 10 & 11, Report on AI Governance Guidelines Development

The Report does refer to copyright concerns associated with AI training and usage. However, it fails to take any concrete step towards addressing a major obstacle faced by the AI-developers and AI-trainers in India. It could have paved the way for fair-dealings exemptions[14] and mining of publicly available text and data for training and R&D purposes when it comes to AI, drawing inspiration from the rich copyright jurisprudence that India currently has, albeit not specifically geared towards AI. Developers and trainers from several other jurisdictions can take such exceptions for granted now[15] and that adds on to the competitive advantage that they tend to enjoy compared to our indigenous counterparts.[16] For instance, under the text and data-mining exceptions laid down under EU law,[17] AI developers are allowed to train on publicly available datasets, though creators whose works form part of these datasets are given the means to opt out.[18] Similarly, under the DPDP Act, 2023 publicly available data can be freely processed by AI companies,[19] which should provide some impetus and latitude to AI companies to work towards technological development in indigenous AI models.[20] However, the lack of a firm stance on this contentious issue may create an environment of uncertainty that could also engender possible infringement allegations against low-risk AI-applications for violating consent requirements. This could result in a chilling effect on all private enterprise aimed at AI development.

Nor does the Report seek to take the other way around and aim to create in conjunction with the evolving data jurisprudence a framework prescribing evaluation, safety standards, security measures and adequate compensation for use of volumes of data for training AI-models. For the purposes of developing an up-to-date regulatory framework in this context, one must focus on enhancing understanding of how Generative AI training and storage works, especially vis-a-vis the copyright jurisprudence in India in relation to the right of

[14] *Copyright Act, No. 14 of 1957*, § 52 (India).
[15] *Directive (EU) 2019/790*, art. 3 & 4.
[16] Imbrie, A., Kania, E., & Laskai, L., *The Question of Comparative Advantage in Artificial Intelligence: Enduring Strengths and Emerging Challenges for the United States*, CTR. FOR SEC. & EMERGING TECH., https://cset.georgetown.edu/research/the-question-of-comparative-advantage-in-artificial-intelligence-enduring-strengths-and-emerging-challenges-for-the-united-states/.; Nestor Maslej et al., *The AI Index 2023 Annual Report*, AI Index Steering Comm., Inst. for Human-Centered AI, Stanford Univ., Apr. 2023, https://aiindex.stanford.edu/report/.
[17] *Supra* note 15.
[18] *Ibid.*
[19] *DPDP Act*, 2023, §3(c)
[20] Adam Buick, *Copyright and AI Training Data—Transparency to the Rescue?*, *J.* INTELL. PROP. L. & PRAC., (2024), https://doi.org/10.1093/jiplp/jpae102., Tajabadi, M., Grabenhenrich, L., Ribeiro, A., Leyer, M., & Heider, D., *Sharing Data With Shared Benefits: Artificial Intelligence Perspective*, J. MED. INTERNET RES., (2023), https://www.jmir.org/2023/1/e47540.

reproduction of copyrighted content, the nuances of the 'fair-use' doctrine and the idea-expression dichotomy that forms the basis of Indian copyright law.[21] One must ensure that a balance is struck between the need to innovate and protecting legitimate interests of the copyright owner.[22]

Recommendations: Strong opt-out mechanisms for copyright holders, such as the ones envisaged under the DPDPAct can be considered for use in this context[23], especially those who released their works publicly before the advent of AI systems and the DPDP Act, lest it continue to instigate further litigation along the lines of *OpenAI v ANI*.[24]

Alternatively, if policymakers do not wish to take a strong stand on fair-use policy, preferring to leave such decisions to the judiciary or legislative bodies, room could be made for alternative modes of procuring and processing data, such as a structured licensing system wherein AI companies must pay copyright holders reasonable fees for training data and also follow data protection & consent guidelines, as mandated in the DPDP Act, 2023.[25]

6. RISK OF REGULATORY CAPTURE AND PRIVACY INFRINGEMENT DUE TO GOVERNMENTAL CONTROL OF TECHNICAL SECRETARIAT.

"*To develop a systems-level understanding of India's AI ecosystem, MeitY should establish, and administratively house, a Technical Secretariat to serve as a technical advisory body and coordination focal point for the Committee/ Group. MeitY should establish and host a*

[21] RG Anand v. Deluxe Films [1978] 4 SCC 118, 140; Eastern Book Company and Ors. v. D.B. Modak, AIR [2008] SC 809; Ghose, Anuttama & Aamir Ali, S.M., *The Principle of Idea-Expression Dichotomy in Copyright Laws: Legal Scenario in India Compared to the Laws of U.S.A. and United Kingdom*, INT'L J. OF EMERGING TECH. & INNOV. RESEARCH, 7(7), (2020), https://ssrn.com/abstract=3722548.

[22] The Chancellor, Masters & Scholars of the University v. Rameshwari Photocopy Services, 233 (2016) DLT 279., Pushpanjali Sood, *Fair Dealing in India: An Analysis vis-à-vis Fair Use in the United States*, J. INTELL. PROP. RTS., 29(6), 560–68 (2024).

[23] *DPDP Act*, §6(4) (2023)

[24] Kalra, Aditya, et al. "*OpenAI Faces New Copyright Case, from Global Book Publishers in India.*" Reuters, 24 Jan. 2025, https://www.reuters.com/technology/artificial-intelligence/openai-faces-new-copyright-case-global-publishers-india-2025-01-24/.

[25] *DPDP Act*, §4, 5 & 6 (2023).

> *technical secretariat that brings in officers on deputation from departments and regulators participating in the Committee/ Group as well as experts from academia and industry.................The proposed secretariat could be staffed by existing MeitY officials as well as lateral hires, young professionals, and consultants. MeitY may form an AI Sub-Group to suggest the form and structure of the proposed secretariat along with a detailed term of reference.*"
>
> -Pages 15 & 16, Report on AI Governance Guidelines Development

The Technical Secretariat that the Report proposes seems to be designed to operate under MeITy's supervision. One should consider what such an overt influence cast by the government may mean for the future operations and practices of the Secretariat -such as its treatment of regulatory concerns posed by AI-based solutions and usage by government organisations as compared to private ones. This is because there is a tendency amongst Government-controlled agencies to prioritize government objectives or the interests of major industry players over independent oversight for the public good, which could further result in a vicious cycle of biased policymaking and enforcement.[26] This phenomena, known as regulatory capture,[27] may hinder innovation and suppress technological development by private AI companies, especially smaller, independent companies in the market.[28]

The extensive government oversight invites further scrutiny, especially in light of the extensive rights granted to the government and governmental departments for processing personal data of individuals, even if data was originally given to some other instrumentality of the government for the provision of some benefit, service or for the grant of certification,[29] or if the government already had such data in digital form, or had it digitized subsequently from, any database, register, book or other document which is maintained by the State or any of its instrumentalities.[30]

[26] Stigler, G. J., "*The Theory of Economic Regulation*," BELL J. ECON. & MGMT. SCI., 2(1), 3-21 (1971).

[27] Dal Bó, E. (2006). "*Regulatory Capture: A Review.*" OX. REV. ECON. POLICY, 22(2), 203-225 (2006).

[28] *Ibid.*

[29] *DPDP Act*, §7(b)(i) (2023).

[30] *DPDP Act*, §7(b)(ii) (2023).

This creates a perfect storm of conditions for a case of regulatory asymmetry where there are stringent data privacy obligations on private enterprises, while government AI projects remain exempt under vague exceptions,[31] and avoid scrutiny.[32] This is especially an area of concern, as historically the judiciary has been a counterbalance to governmental overreach in the Indian context, but the DPDP Act does not provide a mechanism for independent review of state surveillance requests,[33] giving them carte-blanche in many cases. This also has the potential to create a vicious cycle, ala China,[34] where there are faster developments and more fruitful results in government-led AI projects due to paucity of regulatory oversight,[35] which results in greater preference or priority being given to such projects.[36]

More insight is also needed about the exact nature of the relationship that will exist between the proposed Inter-Ministerial Committee and the Secretariat and the T&R of the activities of the Secretariat. In particular, care should be exercised so that the Secretariat does not find itself to be in conflict with the existing sectoral regulators and bodies entrusted with policy formulation on national and regional levels.[37]

Recommendation: Possibilities of using the Secretariat as the foremost standard-setting organisation in this domain may be explored. Alternatively, to prevent the risk of regulatory capture, inter-regulator disputes or arbitrage, the Technical Secretariat could be

[31] *DPDP Act*, §17 (2023).
[32] Karpa, David & Klarl, Torben & Rochlitz, Michael, *Artificial Intelligence, Surveillance, and Big Data* (2021), https://arxiv.org/abs/2111.00992, Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs eds., 2019).
[33] Manwani, Bharat, and Abhiraj Rana. "*The Right to (Pry)-vacy: Understanding India's Dystopian Data Protection Legislation*," N.Y.U. J. Int'l L. & Pol., 12 Feb. 2024, https://nyujilp.org/the-right-to-pry-vacy-understanding-indias-dystopian-data-protection-legislation/.
[34] Karpa, David & Klarl, Torben & Rochlitz, Michael, *Artificial Intelligence, Surveillance, and Big Data* (2021), https://arxiv.org/abs/2111.00992.
[35] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs eds., 2019)., *Parsheera, Smriti, Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?*, Data Governance Network Working Paper No. 05 (Dec. 5, 2019), https://ssrn.com/abstract=3525324.
[36] *Ibid.*
[37] Robert Baldwin et al., *Understanding Regulation: Theory, Strategy, and Practice* (Oxford Univ. Press 2012).

overseen by an independent multi-stakeholder body which would include representatives from academia, civil society, industry, lawmakers etc.[38] This would be more in line with the AI principles advocated for by the OECD, a document that the Report takes support from at multiple junctures.[39]

7. MANDATING STAFFING OF INTER-MINISTERIAL AI COORDINATION COMMITTEE WITH DIVERSE RANGE OF STAKEHOLDERS.

> "*The empowered mechanism should be in the form of an Inter-Ministerial AI Coordination Committee or Governance Group (Committee/ Group). It should bring together the various authorities and institutions that deal with AI Governance at the national level. ………….It may be headed by the Principal Scientific Adviser. Official members could include representatives deputed from MeitY, the NITI Aayog, the Telecommunication Engineering Centre, Bureau of Indian Standards, other departments of the Central Government, as well as sectoral regulators (e.g., RBI, Indian Council of Medical Research, SEBI, IRDAI, Telecom Regulatory Authority of India, etc.). Non-official members could include persons capable of representing the interests of AI developers, AI deployers, data providers, data principals, and end-users – so that the perspectives of the overall ecosystem can be considered. The Committee/ Group should invite external experts for discussions to understand and take on board diverse perspectives."*
>
> -Pages 13 & 14, Report on AI Governance Guidelines Development

The creation of the Inter-Ministerial AI Coordination Committee as suggested by the Report is not a bad move in itself, since the concerns raised by AI-use in a certain sector and the lessons from the same can indeed be used to curate solutions for another sector and

[38] Luciano Floridi, Josh Cowls, Monica Beltrametti et al., *AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, MINDS & MACHINES 28, 689–707 (2018). https://doi.org/10.1007/s11023-018-9482-5.

[39] Organisation for Economic Co-operation and Development (OECD), *Recommendation of the Council on Artificial Intelligence*, OECD Legal Instruments, (accessed Feb. 15, 2025), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449., Organisation for Economic Co-operation and Development (OECD), *National AI Policies*, OECD.AI, https://oecd.ai/en/wonk/national-policies-2 (accessed Feb. 20, 2025).

the Committee may be able to bring down the transaction costs involved in such mechanism because of the presence of stakeholders, both official and non-official, from multiple sectors in it.[40] However, if this stance signifies that the focus of the government is now officially shifting away from carrying out sector-specific research and exploration for AI-based solutions and regulation thereof, then that may be a premature decision to take at this stage.

If such a Committee is to be formed, it should ideally include representatives from a broad range of stakeholders and experts including government officials as well as representatives from academia, industry and civil society, with the focus being on promoting regulatory clarity and consistency, operational efficiency and innovative scalability of the ongoing AI-related developments.[41] In addition, states with proven track record of progress and leadership in this field may also be invited to send their representatives to this committee.

8. CLARITY REQUIRED REGARDING COMPLIANCE WITH AI-INCIDENT REPORTING PROCEDURE AND ALIGNING REPORTING PROCEDURE AND STANDARD RESPONSE IN LINE WITH GLOBAL BEST PRACTICES.

"*To understand the actual incidence of AI-related risks in India, the Technical Secretariat should establish an AI incident database and nurture reporting to it. In the initial stages, the database should receive reports from public sector organisations deploying AI systems (whether directly or through public-private partnerships). Private entities should also be encouraged to voluntarily report AI incidents to the database. The focus should be on defining reporting protocols to ensure confidentiality and to focus on harm mitigation, not fault finding…………………..It is a given that any unlawful activity will be appropriately dealt with through the legal framework. However, the AI incident database should not be started as an enforcement tool. Its objective should not be to penalise people who report AI incidents. Instead, the objective should be to encourage reporting and the learnings*

[40] Floridi, *supra* note 38.

[41] Veale, *supra* note 6; Floridi, *supra* note 38; *See* NATIONAL ARTIFICIAL INTELLIGENCE INITIATIVE ACT OF 2020, USA

should flow back into the ecosystem. Given this, the suitability of CERT-IN taking on the mandate of maintaining an AI incident repository, under the guidance of the Technical Secretariat, may be examined."

-Pages 16 & 17, Report on AI Governance Guidelines Development

The AI-incidents that would form the basis of the database that the Secretariat is supposed to maintain need greater clarity about their definition, categories, treatment, point of intimation, standard operating procedures for reporting etc. The lack of any clarification about the consequences of reporting such incidents, or delay or absence of reporting, may raise operational ambiguity for private parties engaged in AI-development and use.[42] In particular, there should be a sustained and comprehensive effort to build a database of typology of various forms of AI-incidents and their threat assessment based on globally recognised standards and practices.[43]

Recommendation: Standard operating procedures should be developed for reporting such incidents so as to control both over-reporting as well as under-reporting tendencies both of which can be harmful to the industry and society, as well as to prevent duplication of efforts considering that many such incidents may be associated with activities that may lead to those being reported to other existing regulatory authorities and agencies, such as the ones connected with cybersecurity, financial and capital market regulation etc. Perhaps a colour-coded categorisation of incidents based on threat-level and urgency can be formulated for this purpose.[44] The focus should be to encourage voluntary reporting from the stakeholders and build a common database of such incidents so as to develop best practices for risk mitigation. Priority should be given to high-risk sectors for such reporting, including but not limited to sectors with national security implications.[45]

[42] Lee Dixon, Ren Bin & Frase, Heather, *AI Incidents: Key Components for a Mandatory Reporting Regime*, CTR. FOR SEC. & EMERGING TECH., (Jan. 2025), https://doi.org/10.51593/20240023.

[43] National Institute of Standards and Technology (NIST), *AI Risk Management Framework*, NIST, https://www.nist.gov/itl/ai-risk-management-framework (accessed Feb. 8, 2025).

[44] MITRE, *MITRE ATT&CK®: A Knowledge Base of Adversary Tactics and Techniques Based on Real-World Observations*, MITRE, https://attack.mitre.org/, SAMEER GUPTA ET AL., *Guess Who? - A Serious Game for Cybersecurity Professionals*, in *Games and Learning Alliance: GALA 2020*, Lecture Notes in Computer Science, vol. 12517, 41 (I. Marfisi-Schottman et al. eds., Springer 2020), https://doi.org/10.1007/978-3-030-63464-3_41.

[45] Dixon, *supra* note 42.

9. NEED FOR FLEXIBILITY AND CONSTANT UPDATION WITH REGARDS TO ENFORCEMENT OF TRANSPARENCY REQUIREMENTS EXPECTED FROM INDUSTRY STAKEHOLDERS IN LIGHT OF OPAQUE NATURE AND RAPID EVOLUTION OF THE TECHNOLOGY AND RELATED BEST PRACTICES.

> *"Efforts to operationalise the AI Governance principles would require commitment from both the government and the industry. In terms of transparency, this can start by encouraging demonstrable industry self-regulation through examining the adequacy of existing voluntary reports and disclosures being released by current AI developers and deployers (e.g., transparency reports, model cards, etc.)...The voluntary commitments should provide the requisite flexibility to the industry to commit to measures which are meaningful and implementable while providing the much-needed visibility to the regulators and government to the governance measures being implemented. The role of the Technical Secretariat should be to assist these efforts and bring in cross sectoral expertise and a baseline maturity into these commitments."*
>
> -Pages 17 & 18, Report on AI Governance Guidelines Development

The voluntary commitments on transparency that the Report expects from the industry does not seem to take into account issues about the underlying black-box nature of AI development and training that may render adherence to such commitments difficult.[46] Perhaps an industry-wide compilation of similar commitments and voluntary guidelines from other jurisdictions similarly placed in terms of AI-development and growth can be created to facilitate and elicit such commitments in the Indian context.[47]

[46] Jenna Burrell, *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms*, BIG DATA & SOCIETY, 3, 1-12 (2016), https://doi.org/10.1177/2053951715622512.

[47] Personal Data Protection Commission (PDPC) Singapore, *Model AI Governance Framework (Second Edition)*, PDPC, at 26–27, https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf (accessed Feb. 15, 2025)., Personal Data Protection Commission (PDPC) Singapore, *Model AI Governance Framework (Second Edition)*, PDPC, clauses 3.13, 3.16 & 3.17, https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf (accessed Feb. 15, 2025)., Innovation, Science and Economic Development Canada (ISED). *Artificial Intelligence and Data Act (AIDA) Companion Document*, ISED, https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document (accessed Feb. 16, 2025).

Last but not the least, it may not be necessary to completely replace or substitute existing governance mechanisms and structures in favour of some de novo or sui generis model. The best practices applicable in the domain of AI governance and regulation can very well be ideated from existing domains like data protection, cybersecurity, intellectual property and information technology. Initiatives such as regulatory sandboxes can be borrowed from other sectoral regulators and applied mutatis mutandis to the legal structure of AI governance.[48]

Recommendation: The transparency obligations need to be nuanced, keeping in mind the sectoral realities and tiered disclosure norms according to the diverse societal impact of the AI-use cases. The policies drawn up in this regard needs to be above all flexible and subject to regular updation in alignment with the rapidly evolving global standards and industry realities.[49] The digital-by-design approach that the Report talks about is a promising start; however, ideally it should not be imposed on the industry as a whole, rather the different industry players should be allowed to adapt to it over a period of time in a phased manner depending on their capacity and requirements.

[48] Reserve Bank of India (RBI), *Enabling Framework for Regulatory Sandbox*, (Issued on Feb. 28, 2024), https://rbidocs.rbi.org.in/rdocs//PublicationReport/Pdfs/ENABLINGFRAMEWORKFORREGULATORYSANDBOX8640C8810F4C4C38BD3379E58E1C1AE5.PDF, Insurance Regulatory and Development Authority of India (Regulatory Sandbox) Regulations, 2019, F. No. IRDAI/Reg/11/162/2019, (Issued on July 26, 2019).

[49] Financial Conduct Authority (FCA), *Regulatory Sandbox,* FCA, https://www.fca.org.uk/firms/innovation/regulatory-sandbox, (accessed 26 Feb. 2025), Markos Zachariadis and Pinar Ozcan, *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking* ,SWIFT Institute Working Paper No. 2016-001, (June 15, 2017), Available at SSRN: https://ssrn.com/abstract=2975199.