Oct. 12, 2022

To,
Shri. Anand Kumar Singh,
Advisor (QoS)
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
Jawahar Lal Nehru Marg,
New Delhi – 110 002

Subject: Submission of Comments on the Consultation Paper on Leveraging AI and Big Data in Telecommunications Sector

Dear Sir

I am forwarding herewith detailed comments on the Consultation Paper on Leveraging AI and Big Data in Telecommunications Sector issued by TRAI on Aug. 5, 2022. The comments are based on my background in the domain of law with the focus on regulation of techno-legal intersection. Accordingly, the comments are engaging with those issues for consultation which even peripherally relate to the aspects of legal regulations.

The questions are divided under 5 heads and under each of them, question by question comments are provided. The five heads are as follows:

1. Regulatory Framework
2. AI Concepts
3. Regulatory Sandboxes and Lighthouse Projects
4. Academia and industry linkages
5. AI and Big Data in Telecom Sector

The model proposed in these comments for effective regulation of the emerging technologies is highly futuristic. It seeks to adopt a sector-agnostic approach for regulation as the fundamental concerns over the impact of the technologies over individual rights and the harm that the emerging technologies may exert on the human beings may be similar irrespective of the sector they are deployed in. Additionally, the research and development in the technology domain will remain continuous and perpetual occurrence.

Regards

Abhi

Dr. Abhijit Rohi
LL.M. (NUJS, Kolkata), Ph.D. (NLSIU, Bengaluru)
Assistant Professor (Law)
Maharashtra National Law University Mumbai

Comments on TRAI Consultation Paper on Leveraging AI and Big Data

Question-by-question responses

Acknowledgements

I am thankful for the research assistance provided by the following students of BA, LLB (Hons.) programme at NLU Mumbai.
Final Year: Vaishnavi Sharma, Shreenandini Mukhopadhyay
Fourth Year: Ninad Ajane, Aditya Hawaldar
Third Year: Ahsnat Mokarim, Ananya Agarwal, Aparna Bhatnagar
Second Year: Srujan Nirkhee, Harshita Sharma, Kartikeya Kothari, Sameep Baral, Prathamesh Bhutada

Table of Contents

ADDRESSING QUESTIONS ON REGULATORY FRAMEWORK

Questions 11, 12, 17, 18, 31, 35, 37

Question 11: Whether there is a need of telecom/ICT sector specific or a common authority or a body or an institution to check and ensure compliance of national level and sector specific requirements for AI? If yes, what should be the composition, roles and responsibilities of such authority or body or institution? Please justify your response with rationale and suitable examples or best practices, if any.

In recent years with the exponential growth of startups in India,[1] regulation and protection of data has become imperative for the government. It is material to re-iterate that India does not have a comprehensive data protection regime in place, unlike other countries/jurisdictions such as Australia,[2] EU,[3] Brazil,[4] New Zealand,[5] South Korea,[6] etc. Consequently, devising a regulatory structure for AI in the absence of an overarching data protection & regulation regime becomes a challenging task. However, this provides policymakers with the opportunity to appropriately gauge the failures and successes of other regulatory mechanisms in other jurisdictions, especially with regard to AI and BD regulation.

As has been noted,[7] extant issues and concerns about AI technology are not new and already persist in various forms. The primary challenge faced by the proposed authority would be to design and formulate norms and guidelines that enable the effective realization of the fundamental right to privacy across various sectors. This issue gets further exacerbated when one considers the complex and omnipresent usages of AI currently in the private and public sectors, and the accelerating pace at which such systems are designed, adopted, and utlised or anticipated to be utilised by the governments in near future.[8] With the current revamping of the data protection and regulation regime in India and the building anxieties over it,[9] it will be a formidable challenge for the government to come up with an AI regime that (i) is consistent with

[1] MINISTRY OF COMMERCE AND INDUSTRY, *Evolution of Startup India: Capturing the 5-Year story*, available at https://www.startupindia.gov.in/content/dam/invest-india/Templates/public/5_years_Achievement_report%20_%20PRINT.pdf.

[2] The Privacy Act, 1988 (Australia), available at https://www.ag.gov.au/rights-and-protections/privacy#:~:text=The%20Privacy%20Act%201988%20 (Last visited on September 14, 2022).

[3] General Data Protection Regulation (GDPR), available at https://gdpr-info.eu/ (Last visited on September 14, 2022).

[4] General Personal Data Protection Act (LGPD), available at https://lgpd-brazil.info/ (Last visited on September 14, 2022).

[5] Privacy Act (New Zealand), available at https://www.justice.govt.nz/justice-sector-policy/key-initiatives/privacy/ (Last visited on September 14, 2022).

[6] Personal Information Protection Act (PIPA) 2011 (South Korea) available at https://www.privacy.go.kr/eng/laws_policies_list.do (Last visited on September 14, 2022).

[7] NITI AAYOG, *Responsible AI: Approach Document for India: Part 2 - Operationalizing Principles for Responsible AI*, August 2021, available at https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf.

[8] William Eggers, David Schatsky, and Peter Viechnicki, *AI-augmented government Using cognitive technologies to redesign public sector* work, 26, April 2017, available at https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/artificial-intelligence-government.html (Last visited on September 14, 2022).

[9] *Union government rolls back Data Protection Bill,* THE HINDU (2022), available at https://www.thehindu.com/news/national/union-government-rolls-back-data-protection-bill/article65721160.ece. (Last visited on September 14, 2022).

the incoming data protection and regulation law, (ii) is consistent with the international standards, (iii) factors in the social, economic, and political challenges involved with the enforcement and implementation of a proposed AI law.

Exploring regulatory framework alternatives

The OECD has prescribed certain crucial factors while assessing regulatory alternatives. These include the following:[10]

- address clearly specified policy objectives,
- are consistent with other, existing regulations,
- have effective monitoring and compliance mechanisms,
- maximise benefits and minimize costs,
- provide a degree of flexibility where possible to allow the regulated to find the lowest cost way,
- of complying with specified requirements,
- minimise compliance costs – both those borne by regulated entities and the government itself,
- are transparent in their operation and impacts,
- contain appropriate appeals mechanisms.

Co-regulation is a type of regulatory model which consists of a primary regulation, as well as some form of direct participation of stakeholders or their representation. This model seeks to establish a regulatory structure where both private and public sectors (the regulator and the regulated), are actively involved in the regulatory decision-making processes.
As identified by the OECD, while co-regulation involves active participation of stakeholders, it entails explicit governmental involvement, providing the requisite government involvement and legislative backing to effectively enforce and implement the laws, and impose penalties in cases of non-compliance.[11] Considering the sector-agnostic nature of AI and its deep pervasiveness in the public and private sector, co-regulation provides for an effective mechanism for dispute resolution; greater consumer protection; greater willingness by industry stakeholders to abide by the laws and regulations.

Factors to be considered while for an AI regulatory framework

As recognised by the European Commission,[12] the following four factors are to be specifically considered while drafting any regulatory framework for AI:

I. ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;

[10] OECD, *Alternatives to Traditional Regulation,* .4-5*,* available at https://www.oecd.org/gov/regulatory-policy/42245468.pdf.
[11] *Id.*, at 35.
[12] EUROPEAN COMMISSION*, A European approach to artificial intelligence,* 3, available at https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence. (Last visited on September 14, 2022).

II. ensure legal certainty to facilitate investment and innovation in AI;

III. enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;

IV. facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

Accordingly, while preparing a domestic regulatory model for AI, it is important to note the following aspects:

(a) Enabling business and reducing compliance burdens

With the onslaught of regulatory laws and authorities in the recent years, navigating the pathway becomes a humongous challenge for businesses, especially small and medium-sized entities.[13] As the startup ecosystem booms in India, there are veritable challenges identified in terms of the increasing entry barriers to such businesses, anticipating non-compliance and regulatory arbitrage.[14] To combat the same, it is imperative for the authority to ensure that businesses and IT partners understand the technical and legal jargon involved in the various processes. Additionally, it would be beneficial to provide guidance in the form of providing comprehensive toolkits and compendiums to enable a better understanding of the regulatory model and compliance expectations from the proposed AI law.[15]

(b) Regulatory Impact Analysis and stakeholder consultation

Regulatory Impact Analysis (RIA) is an important exercise while policymaking to critically assess the positive and negative effects of proposed and existing regulations and non-regulatory alternatives.[16] Such analysis is primarily based on empirical and scientific analysis, which lets the executive identify the various seen and unseen regulatory challenges and costs.[17] Such an exercise becomes more important considering the technical and unforeseeable challenges involved in new and emerging technologies. The OECD has listed the best practices to be followed while conducting an RIA.[18]

[13] SCIENCE TECHNOLOGY INDUSTRY, REGULATOR, *Regulatory Reform for Smaller Firms,* available at https://www.oecd.org/cfe/smes/2090708.pdf.

[14] Kamesh Shekar, *Building Effective and Harmonised Data Protection Authority- Strategies for Structural Design and Implementation,* THE DIALOGUE, (2020), available at https://thedialogue.co/wp-content/uploads/2022/04/Building-Effective-and-Harmonised-Data-Protection-Authority-Strategies-for-Structural-Design-and-Implementation.pdf.

[15] For additional information, please refer to the answer to question no.37.

[16] OECD ILIBRARY, *Regulatory Impact Assessment: Executive Summary*, available at https://www.oecd-ilibrary.org/sites/7a9638cb-en/1/2/1/index.html?itemId=/content/publication/7a9638cb-en&_csp_=619a2d489e8b70731fae862e094facd9&itemIGO=oecd&itemContentType=book (Last visited on September 14, 2022).

[17] OECD ILIBRARY, *Regulatory Impact Assessment: Background and context*, available at https://www.oecd-ilibrary.org/sites/7a9638cb-en/1/2/1/index.html?itemId=/content/publication/7a9638cb-en&_csp_=619a2d489e8b70731fae862e094facd9&itemIGO=oecd&itemContentType=book (Last visited on September 14, 2022).

[18] OECD ILIBRARY, *Regulatory Impact Assessment: Best practice principles for regulatory impact analysis,* available at https://www.oecd-ilibrary.org/sites/7a9638cb-en/1/2/2/index.html?itemId=/content/publication/7a9638cb-

Furthermore, as has been noted by the OECD, stakeholders' interest and participation is crucial when formulating any regulatory policy for AI; these include citizens, civil society groups, private companies, research organisations and others.[19] These consultations are crucial for understanding the various concerns and interest of stakeholders, and for devising appropriate measures, code of conducts, and largely designing and development AI systems, and diversity of development teams.[20] Accordingly, before any policy is made, and before any specific standards/measures/code of conduct is prepared, it is imperative that the government conducts appropriate stakeholder consultations.[21] Such public consultations would be specifically crucial while conducting an RIA.[22]

(c) Inter-departmental communication, and the need for sector-specific bodies

AI is a sector-agnostic field; it is imperative to consider the cross-sector implications and interlinkages of regulating data, data handling, and data protection. Further, data regulations are scattered across various sectors, regulated by multiple entities by often overlapping and conflicting scopes.[23] Furthermore, the CCI, in its report, has itself identified that there needs to be formal and informal lines of communication between different regulators and that overlapping jurisdictions ought to be harmonised through better regulatory design and improved lines of communication.[24] To enable seamless communication between different regulators and ensure access to sector-specific expertise, it is imperative for the regulatory body to explicitly provide a mechanism for it. It is accordingly critical to synchronise the different regulators, including industry stakeholders, to establish a risk-based framework that identifies specific circumstances when higher standards and additional obligations are required.[25]

(d) Exploring phased approaches towards implementation

en&_csp_=619a2d489e8b70731fae862e094facd9&itemIGO=oecd&itemContentType=book (Last visited on September 14, 2022).

[19] OECD, *An overview of national AI strategies and policies* 7, available at https://goingdigital.oecd.org/data/notes/No14_ToolkitNote_AIStrategies.pdf.

[20] EUROPEAN COMMISSION, *Proposal for a Regulation laying down harmonised rules on artificial intelligence,* 7-16, available at https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.

[21] *Id.*, at 9.

[22] EUROPEAN COMMISSION, *Proposal for a Regulation laying down harmonised rules on artificial intelligence,* Principle 4.4, available at https://www.oecd-ilibrary.org/sites/7a9638cb-en/1/2/1/index.html?itemId=/content/publication/7a9638cben&_csp_=619a2d489e8b70731fae862e094facd9&itemIGO=oecd&itemContentType=book (Last visited on September 14, 2022).

[23] *See* Kamesh Shekar, *Building Effective and Harmonised Data Protection Authority- Strategies for Structural Design and Implementation,* THE DIALOGUE, (2020), available at https://thedialogue.co/wp-content/uploads/2022/04/Building-Effective-and-Harmonised-Data-Protection-Authority-Strategies-for-Structural-Design-and-Implementation.pdf.

[24] COMPETITION COMMISSION OF INDIA, *Market Study On The Telecom Sector In India Key Findings And Observations* 30, February 2, 2021, available at https://www.cci.gov.in/images/marketstudie/en/market-study-on-the-telecom-sector-in-india1652267616.pdf.

[25] *See* Kamesh Shekar, et.al., DPB 2021: *The Data Protection Authority and Coordination with Sectoral Regulators*, The Dialogue-NASSCOM Policy Brief 1-3 (2020), available at https://thedialogue.co/wp-content/uploads/2022/07/DPB-2021-The-Data-Protection-Authority-and-Coordination-with-Sectoral-Regulators.pdf (Last visited on September 14, 2022).

It is in the interest of all stakeholders to actively enable implementation in a way that does not apprehend or anticipate non-compliance. To this end, it is imperative for policymakers to consider a phased approach toward the implementation of any regulatory mechanism, especially considering the disproportionate impact of new regulations on small and medium-sized entities.[26] Phased approaches can be considered in multiple ways, such as the type of business models; the kind of sector the business is engaged in; the kinds of different data dealt with and in what capacity; the size of the business; enforcing certain obligations in a phased manner; etc. With such an approach, businesses that will inevitably be impacted would be able to course-correct sooner and effectively comply with the law.

[26] *See* ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, R*EGULATORY REFORM*
FOR SMALLER FIRMS, available at https://www.oecd.org/cfe/smes/2090708.pdf.

NETRA (National Emerging Technology Regulatory Authority)
A Statutory Authority of the Government of India Committed to Innovating Responsibly

Considering the above assessing factors, we propose the constitution of a co-regulatory body named "**National Emerging Technology Regulatory Authority**" (**"NETRA"**), to oversee the implementation, regulation, and supervision of all AI-related laws and activities in the country. We have identified and analysed the regulatory structure of around 17 domestic regulators across varying sectors to better grasp the extant regulatory models. We have prepared a table with the various regulators; it is annexed as "Annexure A".

Need for statutory authority:

1. To create a responsive, transparent, and accountable public institution committed to Constitutional values in the adoption of emerging technologies
2. To establish an expert, responsible and trustworthy entity entrusted with the task of fueling innovation and investments in the domain of emerging technologies
3. To create a framework for spearheading and channeling the developments in the domain of emerging technologies in a way that is respectful of the fundamental and human rights of all
4. To address effectively present and future challenges due to technological advancements
5. To create an institutional framework for adjudicating disputes in an efficient and timely manner
6. To emphasize the commitment that humans must be in control of emerging technologies and that the technologies are to serve humankind
7. To highlight and showcase India's commitment and preparedness to actively foster responsible innovations in the domain of emerging technologies

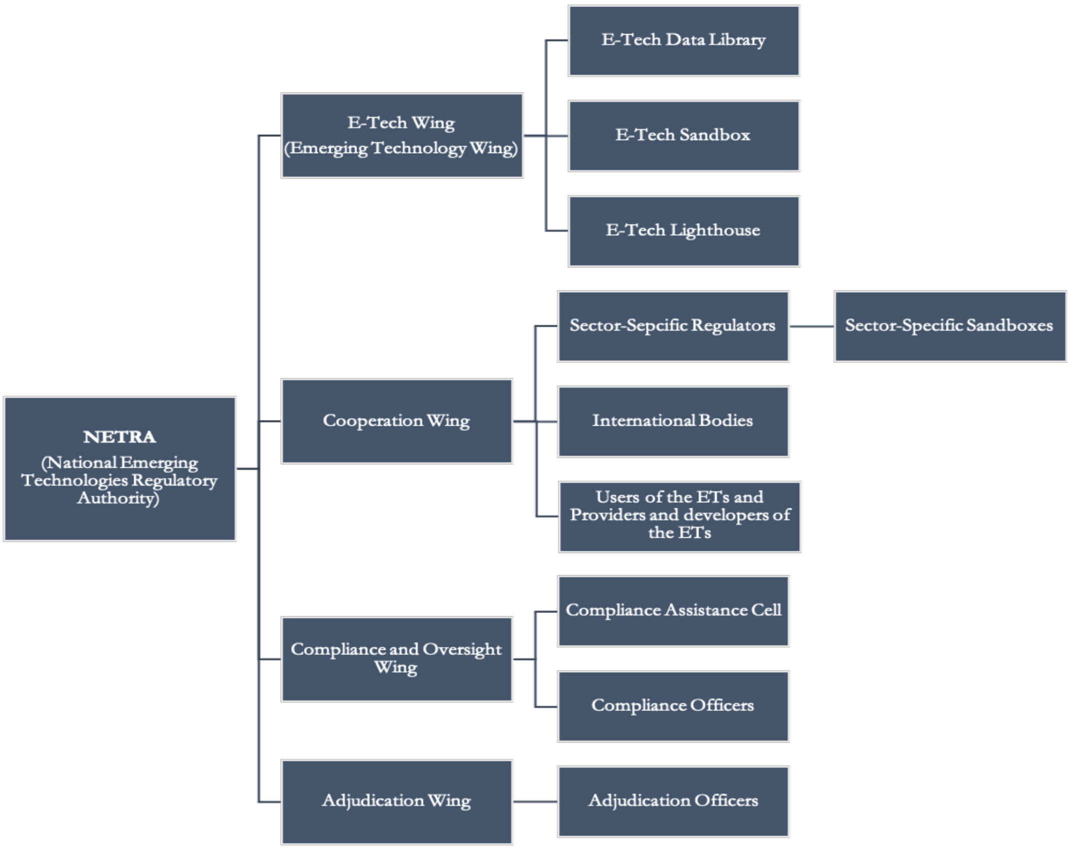
Functions:

- ➔ Monitoring and enforcement
- ➔ Legal, policy and standard setting
- ➔ Inquires, Grievance handling and adjudication
- ➔ Research and awareness

Powers:

- ➔ Issuing Codes of Practice after stakeholder consultations
- ➔ Issuing directions and seeking information
- ➔ Recalling the systems using or deploying emerging technologies
- ➔ Withdrawal of the systems using or deploying emerging technologies
- ➔ Laying down the standards and procedures
- ➔ Securing cooperation between various stakeholders and sectoral regulators
- ➔ Funding research, training, development, and awareness programmes

Proposed organisational structure of NETRA


NETRA
(National Emerging Technologies Regulatory Authority)
E-Tech Wing
(Emerging Technology Wing)
E-Tech Data Library
E-Tech Sandbox
E-Tech Lighthouse
Cooperation Wing
Sector-Sepcific Regulators
Sector-Specific Sandboxes
International Bodies
Users of the ETs and Providers and developers of the ETs
Compliance and Oversight Wing
Compliance Assistance Cell
Compliance Officers
Adjudication Wing
Adjudication Officers

Proposed composition of the main body

Sr. no.	Proposed members	Qualifications
1.	A Chairperson, selected by the Central Government	The individual nominated must be qualified to be a judge of the High Court and/or must have special knowledge or professional experience of at least 15 years in domains of international trade, economics, business, commerce, law, finance, accountancy, management, industry, public affairs, administration, or technology.[27]

[27] This qualification requirement is directly inspired by the composition of the regulatory body under the Competition Act, 2002.

2.	10 domain experts selected by the Central Government; these domains will include: a. Law b. Social sciences c. Technology d. Cyber security e. Economics f. Administration g. Public affairs h. Industry i. Data protection & regulation j. Management	The individuals selected must have special knowledge or considerable professional experience of at least 10 years in their respective fields.

Proposed wings and their roles/responsibilities

- **E-Tech Wing: (Emerging Technology Wing):**

The E-Tech wing is a technical wing of the NETRA which is entrusted with the task of establishing:

  - E-Tech Data Library,
  - E-Tech Sandbox and
  - E-Tech Lighthouse.

These initiatives are proposed to boost innovation and create an eco-system for encouraging participation in the development and deployment of emerging technologies. Based on its experiences and lessons of the sandbox, the E-Tech wing will be able to give inputs for legal and policy affairs, standard settings, codes of practice, and certifications that are relevant to AI.

- **Cooperation Wing:**

Since NETRA is a sector-agnostic Authority, it has to act in coordination with various sectoral regulators. Various sector-specific challenges arising from emerging technologies need to be addressed in collaboration with the expert regulators of that sector. Broader challenges posed due to emerging trends may be similar and can be better addressed by a sector-agnostic Authority, but to deal with sector-specific issues, combined expertise both in the domain of technology and in the respective sector is needed. These sectors may include the healthcare sector; telecom sector; finance, banking, and insurance sector; data protection and regulation sector; education sector; environment sector; agriculture sector; auto-manufacturing assembly and transport sector; etc.

Additionally, the Cooperation Wing has to coordinate seeking opinions of various stakeholders including users, developers, and deployers of emerging technologies. For this purpose, industry-academia linkages in carrying out research, impact analysis, training, etc. to have a skilled workforce is fundamental. The Cooperation Wing must facilitate multi stake-holder deliberations. In order to address the challenges to data protection, the NETRA and Cooperation Wing must work closely with the expert and independent Data Protection Authority of India.

For ensuring India's continued participation and leadership role in developing emerging technologies at the international level, cooperating, and coordinating with various international bodies is highly significant in setting the foundations of future developments collectively. Standardization and interoperability are also two prominent concerns that can be addressed effectively through international cooperation along with the free flow of data for building better quality AI systems.

- **Compliance and Oversight Wing:**

Owing to uncertainties and risks associated with the development and deployment of emerging technologies, some obligations need to be imposed on the developers and deployers. These obligations must emanate from not only the Constitutional guarantees of fundamental rights but also the human rights of the users. These obligations may be precautionary in nature, as it is difficult to regain control over the data once compromised and the automated decision made by the AI systems may result in violations of some rights of the individuals. Accordingly, certain measures such as periodic audits, mandatory periodic submission of reports, record keeping, mandatory security safeguards, transparency requirements, privacy-sensitive precautionary measures including privacy by design and privacy by default measures and data protection impact assessments, etc. must be imposed on the developers and deployers of AI systems. Proportionately adequate obligations imposed will help minimize harm to the users and mitigate the liability of the developers and deployers.

Additionally, in case of any cyber security incident, mandatory breach notifications to the impacted users must be issued as part of an enforcement action supplemented with evaluation and enforcement of the plan of action to mitigate any harm.

Every developer and deployer for the aforementioned purposes must appoint a Compliance Officer who shall serve as a contact person for NETRA. The Compliance Officer will be responsible for adhering to the codes of practice, and standards set forth by NETRA pertaining to accountability, transparency, and explainability along with any other obligations arising from any other law in force in India. For example, obligations may arise under the Data Protection Law, the Information Technology Act, the Consumer Protection Act, etc. The Compliance Officer will be responsible for complying with the directions issued by NETRA from time to time. Any non-compliance or discrepancies found in the periodic audits and reports submitted to NETRA may be forwarded to the Adjudication Wing for further action.

A 'Compliance Assistance Cell' may be established under this Wing. There is a concern that is usually raised about the financial burden involved in undertaking compliances. This burden appears more if the regulator is fashioned as an adversary of the developer or the deployer. However, even though the regulator has the responsibility to secure compliance, it can be considered a cooperative act. The regulator along with developers and deployers have to internalize that being compliant is in everybody's best interest. In order to give effect to the said roles, a Compliance Assistance Cell may be established. The Cell is proposed to provide assistance to the developers in being compliant with the obligations set out in the law, regulations, and rules thereunder. Under the guidance of the trained members of the faculty, with proper legal safeguards in place, students of the law, technology, and management Universities may be permitted to assist the developers and start-ups in emerging technology domains. This will not only secure compliance but also provide students with hands-on training and learning opportunities creating an innovation ecosystem.

- **Adjudication Wing:**

Since there are obligations that are proposed to be imposed on the developers and deployers of AI systems and other emerging technologies, effective enforcement of these obligations stands at the core of a successful regulatory regime. Accordingly, the Adjudication Wing is entrusted with the task of enforcing these obligations and taking necessary action against the non-compliant entities. The Adjudication Wing is proposed to have qualified and trained Adjudicating Officers who will carry out the tasks of conducting detailed inquiries, preparing reports, and imposing civil liability on the non-compliant entity.

The liability imposed by the Adjudicating Officers is in addition to the liability which may be incurred by the non-compliant entity under any other law in India including the Data Protection Law, the Information Technology Act, and the Consumer Protection Act. Even the Adjudication Wing has to work closely with the expert and independent Data Protection Authority of India.

A right to appeal may be granted to an aggrieved party.

Some Additional Aspects:

1. Training, Conferences, and Awareness Programmes:

The periodic training and knowledge-sharing conferences have to be conducted to ensure uniformity and be constantly responsive to the changing nature of the challenges posed by emerging technologies and other technological advancements. Such training and conferences may be organized by Academic Institutions in collaboration with NETRA and technology developers and deployers. Separate and joint training programmes and conferences may be organized for Compliance Officers, Adjudicating Officers, recognised members of the Compliance Assistance Cell, Sectoral regulators, academia, etc. Awareness programmes for the general public may also be arranged as part of public outreach initiatives of NGOs and academic institutions.

The law, technology and management universities and institutions may contribute in developing certain modules for raising awareness among different stakeholders concerning legal requirements and mandated compliances and adoption of technological and management measures.

2. Generation of Funds through CSR:

To incentivise the developers and deployers undertaking any projects and are meaningfully and resourcefully contributing to further the initiatives of the NETRA, their contribution may be treated as their compliance of their statutorily mandated activities as part of corporate social responsibility (CSR).

Question 12: In response to Q.11, if yes, under which present legal framework or law such authority or body or institution can be constituted and what kind of amendments will be required in the said law? Or whether a new law to handle AI and related technologies is a better option? Please justify your response with rationale and suitable examples or best practices, if any.

As elaborated in the answer to question no. 11, the constitution of a new separate statutory authority is proposed with a new, comprehensive law that would specifically regulate, supervise and advocate for emerging technologies. While the introduction of a new regulatory authority would add to the number of regulatory authority stakeholders would have to comply with; it is imperative to do so considering the rising technological complexity and the increasing pervasiveness in private and public sectors, especially with respect to AI.

Question 17: Whether the authority or body or institution as suggested in response to Q.11 may also be entrusted with the task to manage and oversee collection, cataloguing and storage of data? Whether such authority or body or institution needs to be entrusted to generate and make available synthetic data? Please justify your response with rationale and suitable examples, if any.

As was noted by the BN Srikrishna report, the data protection law would form the principal law and minimum threshold for data processing in the country - while other laws could provide stricter and additional compliances none could be inconsistent with the principal law.[28] Considering the same, while the stakeholders wait for the comprehensive data regulation and protection regime, it would be in the interests of the regulators if they are conversing with each other over the nuances of data protection being envisaged by the authorities. Having substantive features that are more lenient in terms of data protection and regulation than what the new data law would provide could invite certain issues once the new data law gets enacted.

Accordingly, the proposed regulatory authority would not be entrusted with managing, and overseeing the collection, cataloging, and storage of data; the incoming comprehensive data law would address such questions at the outset.

Question 18: Whether the legal framework as envisaged in para 3.5.3 and Q.12 should also enable and provide for digitalisation, sharing and monetisation for effective use of the data in AI without affecting privacy and security of the data? Please justify your response with rationale and suitable examples, if any.

Yes, it should. It would primarily be the responsibility of the proposed E-Tech Wing; the modalities would be determined by the regulatory authority after appropriate stakeholder consultations.

Notedly, with the growth and reach of the internet and other advanced technologies, such digitalisation, sharing, and monetisation of data are not limited to business models that are

[28] COMMITTEE OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA REPORT, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians* 98, available at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

exclusively dependent on data, but are also carried out in various forms, ways, and degrees by other conventional businesses that do not seem to be dependent on data. As has been widely noted, enabling digitalisation, sharing, and monetisation for effective use of AI are essential as they improve the predictability and performance of businesses automatically through experience and data, without being manually programmed to do so. Resultantly, data is used and re-used continuously to give a competitive edge to businesses, and overall contribute to competition and innovation in the market.[29]

Question 31: Whether AI/ML developers should launch bounty programs to establish trust in the public about robustness of measures taken by them to protect privacy in their products or solutions? Whether conduction of such programs will help companies or firms to improve their products or solutions? Whether such programs should be conducted under the supervision of the government or an institution established/assigned for this purpose? Please justify your response with rationale and suitable examples, if any.

Yes, it would be beneficial to launch bounty programs under the proposed NETRA's supervision.

Bounty programs have become an essential towards ensuring increased security, not only enabling AI based companies to evaluate their outputs based on explainability and increase overall transparency, but also strengthening the companies' in-house cybersecurity department.[30] Such programs are slowly gaining recognition in India,[31] with the 2016 Facebook report revealing that India is at the top of the list with respect to bounty program payouts.[32] There are already several private companies that have flourishing bounty programs with substantial rewards; these include OLA, McDelivery, PayTM, Yatra, MobiKwik, etc.[33]

The table below lists some of the data-related bounty programs conducted by various jurisdictions, along with a brief description of these programs.

Sr. No.	Regulatory authority	Brief description
1.	India, Unique	Unique Identification Authority of India (UIDAI) has announced a Bug

[29] V Sena & M Nocker, *AI and business models: the good, the bad and the ugly. Foundations and Trends in Technology,* INFORMATION AND OPERATIONS MANAGEMENT 324-397, available at https://eprints.whiterose.ac.uk/182363/3/Sena%20Nocker%20feb%205%202021.pdf.

[30] Gopalani Avi, *How Can Bounty Programs Overcome AI Biases*, August 9, 2021, available at https://analyticsindiamag.com/how-can-bug-bounty-programs-combat-ai-biases/ (Last visited on September 14, 2022).

[31] Anand Murali, *These Modern Day Indian Bounty Hunters Are Making A Killing Hunting (Software) Bugs*, The First post, November 14, 2019, available at https://www.firstpost.com/tech/news-analysis/these-modern-day-indian-bounty-hunters-are-making-a-killing-hunting-software-bugs-7651801.html (Last visited on September 14, 2022).

[32] Available at https://www.facebook.com/notes/1095924270826272/

[33] Harsjeet Sarmah, *Indian Bug Bounty Programs Every White Hat Hacker Can Try*, March 7, 2019, available at https://analyticsindiamag.com/5-indian-bug-bounty-programs-every-white-hat-hacker-can-try/ (Last visited on September 14, 2022).

	Identification Authority of India (UIDAI)	Bounty program for Aadhar to find out any vulnerabilities in its system. There has long been a demand for such an exercise as multiple claims have been made regarding loopholes in the security of Aadhaar data. Calling ethical hackers is one of the great steps from the Indian Government.[34]
2.	Singapore, The Government Technology Agency (GovTech)partnered with HackerOne	The Government Technology Agency (GovTech) launched a new Vulnerability Rewards Programme (VRP) to augment the existing Government Bug Bounty Programme (GBBP) and Vulnerability Disclosure Programme (VDP). Together, the three crowdsourced vulnerability discovery programmes supplement GovTech's suite of cybersecurity capabilities to safeguard the Government's Infocomm Technology and Smart Systems (ICT&SS).[35]
3.	United States, The US Department of Homeland Security (DHS)	The US Department of Homeland Security (DHS) has launched a bug bounty program inviting selected security researchers to test for vulnerabilities in its systems. Dubbed 'Hack the DHS', the program will include three different phases – a pen test, a live hacking event, and a detailed review process. Hack DHS launched in December 2021 with the goal of developing a model that can be used by other organizations across every level of government to increase their own cybersecurity resilience. During the second phase of this three-phase program, vetted cybersecurity researchers and ethical hackers will participate in a live, in-person hacking event. During the third and final phase, DHS will identify lessons learned, including informing future bug bounty programs.[36]
4.	Australia, Department of Premier and Cabinet (DPC)	The South Australian (SA) government is launching a bug bounty program (VENDORIQ) through the Department of Premier and Cabinet (DPC) to drive cyber security researchers in the discovery of weaknesses in the organisation's technology. The DPC revealed that 234 of the SA government's environments have not undergone pentesting in the past three years. The SA government allotted a AU$20 million budget for its cyber defence program in 2021. In 2019, New South Wales created the state's first bug bounty program through the Service NSW digital driver's licence.[37]

[34] UIDAI, *Bug Bounty Program,* available at https://uidai.gov.in/images/Bug_Bounty_Circular.pdf.

[35] GOVTECH SINGAPORE, *New Vulnerability Rewards Programme to test Resilience of Critical Government Systems,* August 31, 2022, available at https://www.tech.gov.sg/media/media-releases/2021-08-31-new-vulnerability-rewards-programme (Last visited on September 14, 2022).

[36] HOMELAND SECURITY USA, *"Hack DHS" Program Successfully Concludes First Bug Bounty Program*, April 2022, available at https://www.dhs.gov/news/2022/04/22/hack-dhs-program-successfully-concludes-first-bug-bounty-program. (Last visited on September 14, 2022).

[37] IBRS, *VENDORIQ: Bug Bounty Program to be Launched by South Australian Government, available at* https://ibrs.com.au/practices/strategy-transformation/bug-bounty-program-to-be-launched-by-south-australian-government. (Last visited on September 14, 2022).

5.	UAE, Cybersecurity Council	The UAE National Cyber Security Council (NCSC) launched on Sunday phase one of the “National Bug Bounty Programme”, which aims to enhance the UAE’s cybersecurity systems, reinforce the country’s leading stature in global competitiveness indexes, as well as engage community members and public and private sector entities in the protection of infrastructure. the programme will initially be piloted by the telecommunications industry, jointly with Etisalat and Emirates Integrated Telecommunications Company (du) in coordination with the Telecommunications and Digital Government Regulatory Authority (TDRA).The initiative aims to promote the culture of cybersecurity and protect the country’s digital transformation and overall achievements in line with the country's leadership directives.[38]
6.	Switzerland, National Cyber Security Centre (NCSC)	Switzerland’s National Cyber Security Centre (NCSC) has announced it is launching a new bug bounty program for the federal government. A pilot project conducted in 2021 saw a total of six IT systems of the Federal Department of Foreign Affairs, FDFA, and the Swiss parliamentary services scanned by ethical hackers for security vulnerabilities. The project returned a total of 10 vulnerabilities, including one classified as critical, seven as medium and two as low. As a result, the program was expanded to include other federal agencies under the leadership of the NCSC.The new security rewards program, which is expected to launch this year, will be managed by Bug Bounty Switzerland AG, which confirmed today (August 3) that it has been awarded the government contract.[39]
7.	European Commission	In 2019, The European Commission announced the EU-FOSSA 2 bug bounty initiative for popular open source projects, including Drupal, Apache Tomcat, VLC, 7-zip and KeePass. The project was co-facilitated by European bug bounty platform Intigriti and HackerOne and resulted in a total of 195 unique and valid vulnerabilities.[40]

Question 35: Whether establishing a system for accreditation of AI products and solutions will help buyers to purchase such solutions or products? If yes, what should be

[38] UAE CYBERSECURITY COUNCIL, ‘*National Bug Bounty Programme*’, August 1, 2021, available at https://www.khaleejtimes.com/local-business/uae-cybersecurity-council-launches-national-bug-bounty-programme. (Last visited on September 14, 2022).

[39] NATIONAL CYBER SECURITY CENTRE, *Federal Administration Procures Platform for Bug Bounty Programs,* available at https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2022/bug-bounty-plattform.html. (Last visited on September 14, 2022).

[40] EU-FOSSA, *EU-FOSSA, Bug Bounties in Full Force,* April 5, 2019, available at https://ec.europa.eu/info/news/eu-fossa-bug-bounties-full-force-2019-apr-05_en#:~:text=The%20EU%2DFOSSA%202%20bug,institutions%2C%20started%20in%20January%202019 . (Last visited on September 14, 2022).

the process of accreditation and who should be authorised or assigned with the task of accrediting such products or solutions? Please justify your response with rationale and suitable examples, if any.

Yes, establishing a system for accreditation of AI products and solutions will be extremely helpful for buyers.

<u>Process:</u> As identified by the OECD, the industry in a co-regulatory framework plays a crucial role in developing the specification of product standards and certification.[41] The proposed co-regulatory framework would ensure that the industry has equal participation, including the process of formulating methods and specifications for accreditation.

<u>Accrediting authority:</u> The proposed E-Tech Wing would oversee accrediting solutions and products. Further, in order to facilitate stakeholder deliberations, the Cooperation Wing would aid these bodies in making the accrediting certifications more lucid, accessible, and available to all stakeholders, including the public. Moreover, regulators might additionally appoint certified organisations to monitor compliance with broad policy requirements or specific technical criteria. However, the proposed body would have to proactively oversee and monitor the operations and processes of such organisations as a matter of precaution. These organisations would have to be publicly listed on the official government websites.

As has been noted by the International Accreditation Forum, accreditation and certification are important as they[42]:

(a) allow Regulators to set overall policy requirements or detailed technical requirements,
(b) reduce uncertainties associated with decisions that affect the protection of human health and the environment,
(c) increase public confidence because accreditation is a recognisable way of demonstrating conformity,
(d) provide confidence on which to base public sector procurement decisions.

Further, as has also been noted by the European Accreditation,[43] the process of accreditation provides a cost-effective means of delivering public services which: are reliable, high quality and safe; support regulatory compliance; imply lower administrative burdens and bureaucracy. Adopting a system for accreditation would invariably benefit the regulators, the industry, and the public at large.

Accreditation and certification are not new concepts to India; we have annexed a table with some of the domestic authorities that accredit/certify/verify products of their sectors as

[41] Glen Hepburn, *Alternatives to Traditional Regulation* 38, available.at https://www.oecd.org/gov/regulatory-policy/42245468.pdf.

[42] INTERNATIONAL ACCREDATION FORUM(IAF), *How does Accredited Certification benefit Regulators?* 3 (2019) available at https://iaf.nu/wp-content/uploads/2021/05/IAF-CMC-19-03-IAF-How-does-Accredited-Certification-benefit-Regulators-9-october.pdf.

[43] EUROPEAN ACCREDITATION, *Accreditation*: *A Briefing For Governments And Regulators*, available at https://european-accreditation.org/wp-content/uploads/2018/10/ea-inf-08.pdf.

"**Annexure B**". While developing the processes for accreditation, the regulators could take learn and take advantage of the experiences and various mechanisms employed by such regulators.

37: Whether there is a need to prepare and publish a compendium of guidance, toolkits and use cases related to AI and BD, to foster adoption in the telecom sector? If yes, what should be the process to prepare such a compendium and who should be assigned this task? Please justify your response with rationale and global best practices, if any.

Yes, there is a need to prepare compendiums, toolkits, etc. These supplemental materials will have to be sector-specific and must address implementation and compliance requirements, helping the stakeholders understand the scope of any AI-specific law; such sector-specific material would ensure willingness of the stakeholders and help prevent non-compliance. Additionally, preparing such supplemental material would invariably enable a smoother enforcement mechanism, with less compliance and regulatory costs. Furthermore, there are several domestic regulators that publish such supplemental material. Many, such as the Goods and Services Tax authorities,[44] the Reserve Bank of India,[45] the Securities and Exchange Board of India,[46] cater to specifically technical sectors, where these supplemental materials are crucial for stakeholders. Similarly, considering the various technical aspects involved in AI, it is imperative to not only provide such materials, but to also provide detailed, sector-specific materials.

Process: Since the supplemental material would have to be sector-specific, it would be in the interests of all stakeholders, including the regulators, to conduct stakeholder consultations to appropriately prescribe specific and detailed guidance notes.

Authority: The proposed Co-operation Wing along with the proposed E-Tech Wing would oversee the formulations and drafting of these materials. Further, in order to facilitate stakeholder deliberations, the Cooperation Wing would aid these bodies in making these supplemental materials more lucid, accessible, and available to all stakeholders, including the public.

The table below lists a few guidance notes, toolkits, etc. published by other jurisdictions or international authorities. The list below demonstrates the various sectors that AI is involved in,

[44] See GST Council, *Explanatory Notes to the Scheme of Classification of Services,* available at https://gstcouncil.gov.in/sites/default/files/Explanatory_notes.pdf.

[45] See RBI, *Guidance Note of Operation of Management Risk,* 2022, available at RBI, https://rbi.org.in/upload/notification/pdfs/66813.pdf.
RBI, *Guidance Notes on Management of Credit Risk and Market Risk,* March, 2002, available at https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=905&Mode=0. (Last visited on September 14, 2022).
RBI, *Guidance Notes for Securitisation Companies and Restructuring Companies,* available at https://rbidocs.rbi.org.in/rdocs/Notification/PDFs/35917.PDF.

[46] See SEBI, *Guidance note to SEBI*, April 24, 2015, available at https://www.sebi.gov.in/legal/regulations/aug-2015/guidance-note-to-sebi-prohibition-of-insider-trading-regulations-2015-issued-on-24-aug-2015-_32384.html.
SEBI, *Guidance Note on Board Evaluation, Jan 05, 2017, available at* https://www.sebi.gov.in/legal/circulars/jan-2017/guidance-note-on-board-evaluation_33961.html. (Last visited on September 14, 2022); SEBI, *Guidance Note on SEBI (Issue and Listing of Municipal Debt Securities) Regulations, 2015,* July 29, 2020, available at https://www.sebi.gov.in/sebiweb/home/HomeAction.do?doListing=yes&sid=1&ssid=85&smid=0 (Last visited on September 14, 2022).

and the necessity of specific and detailed guidance required to appropriately enable AI in those specific sectors.

Sr. No.	**Jurisdiction/international authority**	**Supplemental material**	**Brief description**
1.	UK, Information Commissioner's Office	AI and Data protection risk toolkit[47]	A number of risk areas have been identified, most of which are in line with principles in the UK General Data Protection Regulation, taking in fairness, transparency, security, personalisation, storage limitation, data immunization, lawfulness, accountability, purpose limitation and meaningful human review.[48]
2.	France, Commission nationale de l'informatique et des libertés (CNIL)	AI and GDPR Compliance Note[49] Self-assessment Guide for AI Compliance[50]	CNIL published new resources for AI, aimed at creating a strong AI regulatory framework based on human rights and fundamental values. It has also published various notes on specific issues including on the establishment of a suitable legal basis for processing, data retention period determination, protecting against risks associated with AI models, ensuring transparency and explainability, and the facilitation of data subject rights, among several others. Further, the CNIL offers an analysis grid to allow organizations to assess for themselves the maturity of their artificial intelligence systems with regard to the GDPR; alongside good practices.

[47] ICO UK, *AI And Data Protection Risk Toolkit,* available at https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/ (Last visited on September 14, 2022).

[48] UK'S INFORMATION COMMISSIONER OFFICE, *ICO Unveils Data Protection Risk Toolkit,* May 04, 2022, available at https://www.dataguidance.com/news/uk-ico-launches-updated-ai-and-data-protection-risk.

[49] FRANCE, CNIL, *IA: Comment Être En Conformité Avec Le RGPD?* April 05, 2022, available at https://www.cnil.fr/fr/intelligence-artificielle/ia-comment-etre-en-conformite-avec-le-rgpd (Last visited on September 14, 2022).

[50] FRANCE, CNIL, *Guide D'auto-Évaluation Pour Les Systèmes D'intelligence Artificielle (IA),* April 05, 2022, available at https://www.cnil.fr/fr/intelligence-artificielle/guide (Last visited on September 14, 2022).

3.	Singapore, The Infocomm Media Development Authority	AI Governance Testing Framework & Toolkit[51]	This Toolkit covers technical testing for three principles: fairness, explainability and robustness. The Toolkit provides a "one-stop" tool for technical tests to be conducted by identifying and packaging widely used open-source libraries into a single Toolkit. These tools include SHAP (SHapley Additive exPlanations) for explainability, Adversarial Robustness Toolkit for adversarial robustness, and Fairlearn for fairness testing.
4.	U.S. Department of Health and Human Sciences	Trustworthy AI (TAI) Playbook[52]	Executive Order 13960 "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government" had recognised 9 principles that agencies must follow when designing, developing, acquiring, and using AI in the federal government. The Trustworthy AI (TAI) Playbook is created to assist agencies in satisfying these principles.
5.	Hongkong, Office of the Privacy Commissioner for Personal Data	Guidance on the Ethical Development and Use of Artificial Intelligence[53]	The objectives of this Guidance are to facilitate the healthy development and use of AI in Hong Kong and assist organizations in complying with the provisions of the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO") in their development and use of AI.
6.	Dubai, Digital Dubai	Dubai AI Ethics Principles and Guidelines[54]	The note encompasses a set of AI principles and guidelines, an online self-assessment tool, and a supplementary document that contains directions to resources for technical experts.

[51] INFOCOMM MEDIA DEVELOPMENT AUTHORITY, *AI Governance Testing Framework & Toolkit,* May 25, 2022, available at https://file.go.gov.sg/aiverify.pdf.

[52] U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, *Trustworthy AI (TAI) Playbook*, September 2021, available at https://www.hhs.gov/sites/default/files/hhs-trustworthy-ai-playbook.pdf.

[53] OFFICE OF PRIVACY COMMISSIONER FOR PERSONAL DATA, HONG KONG, *Guidance on the Ethical Development and Use of Artificial Intelligence,* available at https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_ethical_e.pdf.

[54] SMART DUBAI, *AI Ethics Principles & Guidelines,* available at https://www.digitaldubai.ae/docs/default-source/ai-principles-resources/ai-ethics.pdf.

7.	UN Interregional Crime and Justice Research Institute with support from the European Commission	The Toolkit for Responsible Artificial Intelligence Innovation in Law Enforcement[55]	The UNICRI, through its Centre for Artificial Intelligence (AI) and Robotics, signed a new agreement with the European Commission to bolster the development of the Toolkit – a practical guide for law enforcement agencies globally on the use of AI in a trustworthy, lawful, and responsible manner. The Toolkit will contain a collection of practical insights, use cases, principles, recommendations and resources, which will guide law enforcement agencies in their exploration of AI.
8.	World Economic Forum	Artificial Intelligence for Children Toolkit[56] Empowering AI Leadership: An Oversight Toolkit for Boards of Directors[57] Empowering AI Leadership: AI C-Suite Toolkit[58]	The AI for Children Toolkit, produced by a diverse team of youth, technologists, academics and business leaders, is designed to help companies develop trustworthy artificial intelligence (AI) for children and youth and to help parents, guardians, children and youth responsibly buy and safely use AI products. The Oversight Toolkit is created to aid board of directors in overseeing strategy, risk, ethics and social impact, and financial reporting. The AI C-Suite Toolkit provides a practical set of tools to help corporate executives understand AI's impact on their roles, ask the right questions, understand the key trade-offs and make informed decisions on AI projects and implementations

[55] UNICRI and INTERPOL, *The Toolkit for Responsible AI Innovation in Law Enforcement,* available at https://unicri.it/index.php/topics/Toolkit-Responsible-AI-for-Law-Enforcement-INTERPOL-UNICRI (Last visited on September 14, 2022).

[56] WEF, *AI for Children,* March, 2022, available at https://www3.weforum.org/docs/WEF_Artificial_Intelligence_for_Children_2022.pdf.

[57] WEF, *Empowering AI Leadership, 2020,* available at https://www3.weforum.org/docs/WEF_Empowering-AI-Leadership_Oversight-Toolkit.pdf.

[58] WEF, *Empowering AI Leadership AI C-Suit Toolkit, January 2022, available at* https://www3.weforum.org/docs/WEF_Empowering_AI_Leadership_2022.pdf.

9.	(International Criminal Police Organization (INTERPOL)	Artificial Intelligence Toolkit	The Toolkit will offer practical guidelines for the development, procurement and deployment of AI, ensuring it is used in the most appropriate and responsible way and that citizens' rights are protected. Law enforcement agencies across the world will be able to access the knowledge and resources needed to tap into the positive potential of AI, make informed decisions, and reduce possible related risks.

ADDRESSING QUESTIONS ON AI CONCEPTS

Questions 4, 8, 9, 10, and 19(b)

Question 4: Do you think that a number of terminologies such as Trustworthy AI, Responsible AI, Explainable AI etc. have evolved to describe various aspects of AI but they overlap and do not have any standardised meanings? If yes, whether there is a need to define or harmonise these terms? Please justify your response with rationale and global practices, if any.

Trustworthy AI is a term used to describe AI that is lawful, ethically adherent, and technically robust. It is based on the idea that AI will reach its full potential when trust can be established in each stage of its lifecycle, from design to development, deployment and use.[59]

Responsible AI is the practice of designing, developing, and deploying AI with good intention to empower employees and businesses, and fairly impact customers and society—allowing companies to engender trust and scale AI with confidence.

Explainable artificial intelligence (XAI) is a set of processes and methods that allows human users to comprehend and trust the results and output created by machine learning algorithms. Explainable AI is used to describe an AI model, its expected impact and potential biases. It helps characterize model accuracy, fairness, transparency and outcomes in AI-powered decision making. Explainable AI is crucial for an organization in building trust and confidence when putting AI models into production. AI explainability also helps an organization adopt a responsible approach to AI development.

There is an overlap between Trustworthy AI and Responsible AI as both of them heavily rely on Ethics. They don't have standardized meaning but they have general meaning and are open to interpretation. There is definitely a need to harmonize the definitions as this will help us in the future to make entities dealing with AI legally liable for their actions and make sure it is used for mankind's betterment

Question 8: Whether risks and concerns such as privacy, security, bias, unethical use of AI etc. are restricting or likely to restrict the adoption of AI? List out all such risks and concerns associated with the adoption of AI. Please justify your response with rationale and suitable examples, if any.

Risks and concerns associated with the usage of AI can be categorised as sector specific and sector agnostic. Part (a) of this response shall specifically deal with the technical risks and

[59] Requirements for technology to be trustworthy AI, https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1.html

concerns associated with the adoption of AI in the telecom sector. Part (b), (c) and (d) of this response shall deal with the threats to privacy and security and the proliferation of bias that may manifest due to the application of AI in different domains.

(a) Risks specific to the telecommunications ('telecom') sector:

(i) In AI-based systems, it is often difficult to determine the process by which the system delivers an output based on the data fed to it. In the telecom sector, this problem is exemplified by the 'covariance shift'. A covariance shift takes place when an anomaly detection system detects a new flow of traffic from, for example, a browser launched to streamline HTTPS requests. It takes place when the nature of the data changes. This means that the data on which a model is initially trained is no longer representative. The anomaly detection system is trained to detect any suspicious traffic from the network and block it. Since there is a new flow of traffic, an AI-enabled anomaly detection system may automatically block the browser.

(ii) AI-based systems are vulnerable to unpredictability. This is because AI systems may not be deterministic. Determinism means that when an ordinary algorithm is run twice on the same parameters, it produces the same results every time. However, some algorithms use random sampling methods like the Bayesian methods, and as a result of the parameters being different, the result produced may not be the same if the algorithm is run for more than one time. In the telecom sector, AI systems can figure out the best configuration to embed virtual network components in physical infrastructure. Engineers use a Monte Carlo Tree Search to determine the best configuration. However, a Dutch Radiocommunications Agency report says that, due to the use of sampling, "it can never be guaranteed that the same configuration will be suggested twice, given the same environmental factors. Testing can therefore only provide some level of certainty how the model will behave in different situations. In addition, because the best configuration is not known in advance, it is not possible (for a human being) to verify whether the AI system indeed managed to come up with the best configuration." [60]

(iii) It is difficult to affix responsibility when the AI system malfunctions. In the telecom sector, the AI system is trained by the supplier and used by the operator. The training is done by using data from other telecom networks. When an AI system goes wrong or it malfunctions, it will be difficult to affix responsibility because it may affect key performance indicators (KPIs) not specified in the contracts between the supplier and the operator.

(iv) Telecom operators are faced with the problem of incomplete and unorganised datasets. Having a standardised dataset is a key indicator in the success of machine learning algorithms. Network data includes "flows, logs and KPIs" and there is no standard way to combine them into standard datasets. [61]

(b) Risk to privacy by the usage of AI: Data is the lifeblood of AI. Use of artificial intelligence in various systems can enable processing of vast amount of data to make predictions and decisions which, otherwise, would be the function of human intelligence. The amount of data generated from users is enormous and artificial intelligence can be employed to create 'data

[60] Dutch Radiocommunications Agency, *Managing AI use in telecom infrastructures* (2019) Available at BRC194-2020-vdvorst-ai-telecom.pdf (tue.nl) (Last visited September 16, 2022)

[61] Heavy Reading, James Crenshaw *AI in Telecom Operations: Opportunities & Obstacles* (2018) Available at: AI in Telecom Operations: Opportunities & Obstacles (guavus.com) (Last visited on September 8, 2022)

profiles' of the 'data subjects' which offers companies a treasure trove of information to manipulate and influence the user. This leads to the loss of information privacy. Informational privacy refers to the right to control over the flow of personal information, which includes personal information either in our possession or shared with others confidentially.[62] 'Private information' may include health data, biometric data, government records, internet browsing activity, locational history etc. Other forms of privacy to which AI can pose a risk includes decisional privacy (autonomy). Privacy is risked by the usage of AI in some of the following ways:

(i) Loss of anonymity: Anonymization of data is the stripping of personally identifiable information so that the original source cannot be identified. Artificial intelligence has the capability to re-identify anonymized data. For example, a study on credit card data showed that metadata pertaining to credit card records can be uniquely re-identified by up to 90% accuracy, and that women were more susceptible to re-identified than men.[63]

The ability of AI to re-identify data is especially likely to restrict the use of AI in the healthcare sector. The use of AI in the healthcare sector has grown by leaps and bounds. Today, AI is used in radiology to analyse diagnostic imagery. In India, Manipal Hospitals group has partnered with IBM to implement IBM's AI technology (Watson for Oncology) for cancer patients. However, a study showed that even when healthcare information is fully anonymized, yet it is possible to reidentify 85.6% of adults and 69.8% of children in a physical activity cohort study, "despite data aggregation and removal of protected health information". [64] A 2019 study showed that, using a 'linkage attack framework' can successfully link online health data to real world people, thereby highlighting the risks to patient privacy. [65]

(ii) Loss of autonomy: Autonomy refers to "a set of diverse notions including self-governance, liberty rights, privacy, individual choice, liberty to follow one's will, causing one's own behaviour, and being on person."[66] Autonomy may affect the scope of discretion left to the individual in the decision-making process since the individual may feel compelled to accept the decision made by the system enabled by artificial intelligence. An example of how AI affects decisional privacy can be seen in the use of personal digital assistants (also known as 'digital butlers') such as Amazon's Alexa and Google Assistant. Reliance on these 'digital butlers' may cause 'behavioural discrimination' on the basis of the information received from the user. This information may include general interests, reservation price, shopping habits etc. Behavioural discrimination may compel the user to buy the products that the user wouldn't want usually, and hence, distort the

[62] Daniel J. Solove & Neil M. Richards, Privacy's Other Path: *Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007).

[63] Yves-Alelexandre de Montjoye et al., Unique in the Shopping Mall: *On the Reidentifiability of Credit Card Metadata*, 347 SCI. 536 (Jan. 30, 2015),

[64] Na L, Yang C, Lo CC, Zhao F, Fukuoka Y, Aswani A. Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning. JAMA Netw Open. 2018;1(8):e186040.

[65] Ji S, Gu Q, Weng H, Liu Q, Zhou P, He Q, Beyah R, Wang T. De-health: all your online health information are belong to us. arXiv preprint. 2019. https://arxiv.org/abs/1902.00717.

[66] Tom L. Beauchamp & James F Childress, *Principles of Biomedical Ethics* 67-68 (1989)

options available to the user thereby directly affecting the decision-making process of the user by limiting the scope of options shown to the user.[67]

(b) Security risks in AI usage: The use of AI in surveillance and cybersecurity may pose a threat to national security as a whole since "adversaries may systematically feed disinformation to AI surveillance systems, essentially creating an unwitting automated double agent".[68] A threat to cybersecurity owing to the use of AI can be seen in the use of 'artificial agents'. These artificial agents include advanced malware which have the capacity to manipulate information. AI run malware detection systems may themselves be vulnerable to security risks owing to AI systems' *data diet vulnerability* - which means that the performance of AI is dependent on the quality of data that is fed to it. [69]Studies have shown the viability of such training set poisoning attacks for machine-learning–based malware detection systems.[70] This is essentially, data poisoning, which is the contamination of data used to train the AI/ML system. Data poisoning could potentially be used to increase the error rate of the AI/ML system or to potentially influence the retraining process. Some of the attacks in this category are known as "label-flipping" and "frog-boil" attacks.[71]. Other threats to security (in general) include adversarial inputs, which are malicious inputs designed to bypass the AI classifier in cases where the AI system is dependent on input from an external system. [72]

A threat to domestic security may be posed by algorithms by the creation of "filter bubbles" on the internet.[73] It is argued that the close interplay of personalisation of the content consumed on the internet (for example, news content), "demographic hypersegmentation, our cognitive biases, and the closed nature of our online social media platforms may result in echo chambers that amplify misinformation".[74] News curating algorithms play a significant role in the aforesaid, though there is no evidence that algorithms can be 'trained' deliberately to create 'filter bubbles' and amplify misinformation. [75]

[67] Stucke, Ezrachi "*Who wouldn't want a Digital Butler*" (2017) Available at Who Wouldn't Want a Digital Butler? – Berkeley Technology Law Journal (btlj.org) (Last visited on September 16, 2022)

[68] Osoba, Osonde A. and William Welser IV, *The Risks of Artificial Intelligence to Security and the Future of Work*. RAND Corporation (2017) available at https://www.rand.org/pubs/perspectives/PE237.html. (Last visited on September 14th 2022)

[69] Osoba, Osonde A., and William Welser, An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence, RAND Corporation, RR-1744-RC, 2017. https://www.rand.org/pubs/research_reports/RR1744.htm (Last visited 11th September 2022)

[70] Biggio, Battista, Blaine Nelson, and Pavel Laskov, "*Poisoning Attacks Against Support Vector Machines*," Proceedings of the 29th International Conference on Machine Learning, Cornell University (2012) available at https://arxiv.org/abs/1206.6389v1 (Last visited on 11th September 2022)

[71] AI Artificial Intelligence/Machine Learning Risk & Security Working Group (AIRS),, *Artificial Intelligence Risk & Governance* (December 11, 2020) available at .Artificial Intelligence Risk & Governance - Artificial Intelligence for Business (upenn.edu) (Last visited on September 16, 2022)

[72] *Id.*

[73] *See generally* Pariser, Eli, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, (2011)

[74] Tufekci, Z., "*As the Pirates Become CEOs: The Closing of the Open Internet*," Daedalus, Vol. 145, No. 1, 2016b, pp. 65–78.

[75] Dewey, Caitlin, "*Facebook Has Repeatedly Trended Fake News Since Firing its Human Editors*," Washington Post (October 12, 2016), available at https://www.washingtonpost.com/news/the-intersect/wp/2016/10/12/facebookhas-repeatedly-trended-fake-news-since-firing-its-human-editors/?utm_ term=.6c3ecb67d0d7 (Last visited 13th September 2022)

(c) The risk of bias in the usage of AI: Bias akin to that exhibited by humans may be exhibited by artificial intelligence as well. Bias can be 'learned' by the AI-powered system / algorithm if the training provided is inadequate. [76]

An example of the same can be cited from a study conducted by researchers at Princeton University, wherein a statistical MLAG (machine learning algorithm) was deployed to determine the context of certain words in large volumes of text. It was found that female names were associated with stereotypically familial terminology, and African-American names were associated with 'unpleasant' words. These were hidden or implicit biases which the MLAG had learnt due to inadequate training, even if the data set fed to the MLAG may not have revealed such implicit biases to human readers.[77]

If the training data poorly represents the target population or is chosen carelessly, training can directly create harmful learned biases. For example, researchers at Microsoft faced a problem where its facial emotion recognition technology demonstrated learned bias towards the children, elderly and the minorities. The inference drawn was that "Poor representation of people of different ages and skin colors in training data can lead to performance problems and biases". [78]

AI-powered systems have also demonstrated 'historical bias'. A telling example of the same is the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) used in the United States. It is used to predict reoffending risk in convicted criminals. The COMPAS has been shown to have disproportionately categorised African Americans at a higher risk of reoffending (twice that of White Americans) leading to great inaccuracy. In this case, bias is created by selective targeting over a period of time, such as from crime reports being disproportionately from lower-income neighbourhoods with high concentration of minorities.[79]

(d) Risk to democratic systems: The use of artificial intelligence poses risks to the functioning of democratic systems, particularly elections. In the United States, social media algorithms on platforms such as Facebook have been found to have influenced electoral outcomes. In an experiment conducted by Facebook in 2010, Facebook users were shown the news of their friends having voted that day, and this led to an increase in overall voter turnout " by prompting those who received the news to vote in greater numbers, that it could hypothetically affect election results".[80] Although this experiment was conducted to encourage greater participation in elections, it can be argued that nefarious manipulation of AI for swinging election outcomes is very much possible by design.

'Fake news' (including disinformation) - i.e.topical content that is fabricated, distorted, misleading or taken out of context, which is commonly distributed online and often "micro-

[76] Fuchs, Daniel J.. "*The Dangers of Human-Like Bias in Machine-Learning Algorithms.*" Missouri S&T's Peer to Peer 2 (1) available at https://scholarsmine.mst.edu/peer2peer/vol2/iss1/1

[77] Caliskan, A., Bryson, J., & Narayanan, A. *Semantics derived automatically from language corpora contain human-like biases.* Science 356(6334) (2017), pp. 183-186, doi: 10.1126/science.aal4230

[78] Howard, A., Zhang, C., & Horvitz E. (2017). *Addressing bias in machine learning algorithms: A pilot study on emotion recognition for intelligent systems.* 2017 IEEE Workshop on Advanced Robotics and its Social Impacts (ARSO), pp. 1-7, doi: 10.1109/ARSO.2017.8025197

[79] Temming, M. (2017). Machines are getting schooled on fairness. ScienceNews, 192(4), pp. 26, Retrieved from https://www.sciencenews.org/article/machines-are-getting-schooledfairness.

[80] Jonathan Zittrain, *Engineering an Election: Digital Gerrymandering Poses a Threat to Democracy*, 127 HARV. L. REV. F. 335 (2014)

targeted" to affect a particular group's opinions is also a key threat to the functioning of a healthy democracy since the decision-making process of the citizenry gets manipulated by the dissemination of 'facts' which are wrongly represented out of context. Professor Mireille Hildebrandt explains the scale and scope that can create disinformation problems in social media platforms:

"Due to their distributed, networked, and data-driven architecture, platforms enable the construction of invasive, over-complete, statistically inferred, profiles of individuals (exposure), the spreading of fake content and fake accounts, the intervention of botfarms and malware as well as persistent AB testing, targeted advertising, and automated, targeted recycling of fake content (manipulation)."[81]

Professor Hildebrandt further explains that "'data-driven systems parasite on the expertise of domain experts to engage in what is essentially an imitation game. There is nothing wrong with that, unless we wrongly assume that the system can do without the acuity of human judgment, mistaking the imitation for what is imitated". This essentially outlines the dangers of AI failing to process 'false positives'. This is one of the reasons why the European Parliament emphatically states that "Limiting the automated execution of decisions on AI-discovered problems is essential in ensuring human agency and natural justice: the right to appeal."[82] It emphasises on human intervention to weed out 'false positives' because AI powered systems may label some content as disinformation where in fact it could lead to transgression of the freedom of speech and expression. This is despite technology giants such as Facebook claiming that "'its AI tools—many of which are trained with data from its human moderation team—detect nearly 100 percent of spam, and that 99.5 percent of terrorist-related removals, 98.5 percent of fake accounts, 96 percent of adult nudity and sexual activity, and 86 percent of graphic violence-related removals are detected by AI, not users." Such claims were challenged in a 2018 study where researchers have claimed that trained algorithmic detection of fact verification may never be as effective as human intervention, with serious caveats (each has accuracy of only 76%). [83]

The use of AI in a variety of domains, as exemplified by the examples cited in the discussion hereinabove, gives us a area-specific view of the risks posed by AI. Patient privacy for example, is threatened by the use of AI owing to its capability of reidentifying data - hence, use of AI in the healthcare sector may be limited. Furthermore, the demonstration of historical bias in AI tools used by the criminal justice system is also an indicator of the limitations of AI. The use of AI in fake news and disinformation detection, though promising, has its inherent limitations owing to a lack of application of human judgment. All of these examples, as well as others discussed hereinabove, highlight the possible violations of the right to privacy, impair protection against discrimination, endanger the security of the nation against extraneous and intraneous forces and threaten the stability of the democratic system by manipulating electoral system and disinformation. Hence, these risks and concerns are likely to restrict the use of AI in all the aforementioned areas.

[81] Hildebrandt, M. '*Primitives of Legal Protection in the Era of Data-Driven Platforms*', 2 Georgetown Law Technology Review 253 (2018)

[82] European Parliamentary Research Service, European Science - Media Hub, "*Regulating disinformation with artificial intelligence"* (2019) Available at EPRS_STU(2019)624279_EN.pdf (europa.eu) (Last visited September 12, 2022)

[83] Perez-Rosas, V., Kleinberg, B. Lefevre, A. and Mihalcea, R. *Automatic Detection of Fake News*, (2018) Available at http://web.eecs.umich.edu/~mihalcea/papers/perezrosas.coling18.pdf (Last visited on 15th September 2022)

Question 9: What measures are suggested to be taken to address the risks and concerns listed in response to Q.8? Which are the areas where regulatory interventions may help to address these risks and concerns? Please justify your response with rationale and suitable examples, if any.

The risks listed under the previous question (i.e. Question 8) can be mitigated by the adoption of following measures:

(A) General Measures: These general measures are suitable for implementation for business organisations involved in developing AI-powered systems:

(I) Oversight Mechanisms: An oversight mechanism may begin "with the creation of an inventory of all AI systems employed at the organization, the specific uses of such systems, techniques used, names of the developers/teams and business owners, and risk ratings – measuring, for example, the potential social or financial risks that may come into play should such a system fail".[84] Oversight mechanisms could also be implemented in the form of data quality checks - i.e. ensuring that the quality of training data used is optimal enough to minimise the potential risks for an AI powered system running on this data.

(II) Drift monitoring: Drift refers to change in the relationship between the target variables and the individual variables over the period of time. Drift may lead to poor model accuracy, for example. Monitoring may provide insight into the "accuracy drift" of the data. Monitoring could also assess if input data significantly deviates from the model's training data, which could help inform the identification of "data drift."[85]

(III) Mitigation of bias in AI: This can be achieved by:

1. Responsible algorithm development: These include measures such as:
    a) Human-in-the-loop: Ensuring human intervention on high risk AI applications;[86]
    b) Conducting internal and external audits of the AI system
    c) Development of fairness toolkits [87]
2. Responsible dataset development: These includes measures such as:
    a) Broader training data sets to remove selection bias and sampling bias;
    b) Assess existing datasets to check for over-/ under-representation of certain identities, underlying inequities that reflect reality but are ultimately problematic, and address privacy concerns.[88]

The aforementioned measures may be best implemented by regulators for the benefit of the organisations in the form of a set of general recommendations on best practices to be adopted by businesses.

[84] *Supra* note 12

[85] *Id.*

[86] Genevieve Smith and Ishita Rustagi "*Mitigating Bias in Artificial Intelligence: An Equity Fluent Leadership Playbook*" Berkeley Haas Center for Equity, Gender and Leadership (July 2020)

[87] *See* IBM's's Fairness 360 toolkit available at https://github.com/IBM/AIF360 and Microsoft's FairLearn available at https://fairlearn.ai/

[88] *Id.*

(B) Establishing risk management frameworks: Risk management frameworks are mainly aimed towards developers, and are a handy tool for regulators and policy-makers - the aim (of the regulators and policy-makers) is to make sure that the developers take into account the risks and concerns associated with the usage of AI while developing an AI powered system; and address them adequately. In risk impact assessments, higher the risk associated with the use of AI, more stringent the measures prescribed for developers. Usually, when there are low level risks in the usage of AI, minimal oversight is prescribed. But for higher levels of risks, greater human intervention is prescribed. Risk and algorithmic impact assessments assess risk based on the purpose of the system and the quality of data used. The following risk and algorithmic impact assessment frameworks were found noteworthy:

(I) Directive on Automated Decision Making, Canada (the 'Directive'):

The Directive is meant primarily for public agencies looking to utilise AI. The Directive's salient feature is that it provides for an Algorithmic Impact Assessment (AIA), which is an online tool provided to determine the impact level of an automated decision-system. It is composed of 48 risk and 33 mitigation questions. Assessment scores are based on many factors, including systems design, algorithm, decision type, impact and data. AIA is mandatory.

The Directive prescribes the following requirements:

1. Quality assurance:
    a) Data quality should be relevant, accurate, up-to-date[89].
    b) AI powered systems should provide for human intervention [90]
2. Transparency -
    a) includes provision of prior notice stating that the decision rendered by the system utilises automated decision making; [91]
    b) explainable AI - i.e. explanation of how and why the decision was made should be explained to the users; [92]
    c) right to access and test the automated decision making system is reserved with the Government of Canada;[93]
    d) source code should be released.[94]
3. Impact Assessment levels: Levels I to IV are prescribed (I being the lowest impact and IV being the highest impact). Risks are mapped in relation to: the rights of individuals or communities,the health or well-being of individuals or communities,the economic interests of individuals, entities, or communities and the ongoing sustainability of an ecosystem.For higher level impacts, specifications for a system may be needed to be published in a peer reviewed journal.[95]

[89] Directive on Automated Decision Making 2019 (Canada) 6.3.3
[90] Directive on Automated Decision Making 2019 (Canada) 6.3.9
[91] Directive on Automated Decision Making 2019 (Canada) 6.2.1
[92] Directive on Automated Decision Making 2019 (Canada) 6.2.3
[93] Directive on Automated Decision Making 2019 (Canada) 6.2.5.2.
[94] Directive on Automated Decision Making 2019 (Canada) 6.2.6
[95] Directive on Automated Decision Making 2019 (Canada) Appendix B

(II) Opinion of the Data Ethics Commission, Germany:

1. The Opinion of the Data Ethics Commission, Germany proposes a risk-based approach to mitigate the risks associated with automated decision making systems powered by artificial intelligence, with specific focus on algorithmic systems.
2. It provides for the categorization of algorithmic systems for the purposes of determining the risk associated with each category, based on the level of influence the algorithm has over the decision rendered by an automated decision making system:
   a) Algorithm-driven: Decisions which are driven by algorithms with limited scope for human intervention;
   b) Algorithm-based: Decisions which are based on the information provided by the algorithm and the decisions are entirely taken by humans;
   c) Algorithm-determined: Decisions which are automatically rendered by the algorithmic system without human intervention.[96]
3. Principles prescribed for risk impact and algorithmic impact:
   a) Human-centred design;
   b) Compatibility with core societal values;
   c) Sustainability;
   d) Quality and performance;
   e) Transparency and explainability
   f) Accountability
   g) Robustness and security
   h) Minimisation of bias and discrimination[97]
4. Risk assessment levels ('criticality pyramid'):

a) Level 1 applications are associated with zero or negligible potential for harm, and it is unnecessary to carry out special oversight of them or impose requirements other than the general quality requirements;[98]

b) Level 2 applications are applications with some potential for harm. Measures prescribed: Transparency obligations, publication of a risk assessment, monitoring procedures - i.e. disclosure obligations towards supervisory bodies, ex-post controls and audit procedures.[99]

c) Level 3 applications are with regular or significant potential for harm. Measures prescribed - ex-ante approval procedures;[100]

d) Level 4: Applications with serious potential for harm. Measures prescribed:
   - publication of information on the factors that influence the algorithmic calculations and their relative weightings
   - the pool of data used and the algorithmic decision-making model;
   - an option for "always-on" regulatory oversight via a live interface with

[96] German Federal Ministry for Justice and Consumer Protection, *Opinion of the Data Ethics Commission*, October 2019 available at http://bit.ly/373RGqI. p. 17
[97] *Id.* at p.18
[98] *Id.*
[99] *Id.*
[100] *Id.*

the system[101]

e) Level 5: Applications with an untenable potential for harm. Measures prescribed: Complete or partial ban[102]

(III) Proposal for laying down harmonised rules on artificial intelligence (Artificial Intelligence Act):

1. Regulatory approach: The proposal aims to regulate high risk AI applications only, and proposes a code of conduct for low risk AI applications.[103]
2. Risk management system: For the management of risk associated with high risk AI systems, Article 9 of the proposed AI Act proposes the following steps:
   a) identification and analysis of the known and foreseeable risks associated with each high-risk AI system; [104]
   b) estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse; [105]
   c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;[106]
   d) adoption of suitable risk management measures[107]
3. Risk management measures: The AI Act provides guidance to providers on the risk management measures to be adopted. These guidelines include:
   a) Elimination of the risk wherever possible;[108]
   b) If risk cannot be eliminated, then adequate mitigation measures to be employed;[109]
   c) Where there is possibility of its misuse, or there is a possibility of risk when it is used as per its intended usage, then adequate information is to be provided to the users on such risk. [110]
4. Transparency and Information to the Users: The following information is required to be provided to the users:
   a) The identity and the contact details of the provider and, where applicable, of its authorised representative;[111]
   b) Intended purpose of the high risk AI system;[112]
   c) Level of accuracy and robustness;[113]
   d) Future potential risks of misuse; leading to endangerment of health and

[101] *Id.*

[102] *Id.*

[103] European Commission, *Proposal for a Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts* COM(2021) 206 final, p.9

[104] Artificial Intelligence (AI) Act proposal, Art. 9.2 (a)

[105] Artificial Intelligence (AI) Act proposal, Art. 9.2 (b)

[106] Artificial Intelligence (AI) Act proposal, Art. 9.2 (c)

[107] Artificial Intelligence (AI) Act proposal, Art. 9.2 (d)

[108] Artificial Intelligence (AI) Act proposal, Art. 9.4 (a)

[109] Artificial Intelligence (AI) Act proposal, Art. 9.4 (b)

[110] Artificial Intelligence (AI) Act proposal, Art. 9.4 (c)

[111] Artificial Intelligence (AI) Act proposal, Art. 13.3 (a)

[112] Artificial Intelligence (AI) Act proposal, Art. 13.3 (b) (i)

[113] Artificial Intelligence (AI) Act proposal, Art. 13.3 (b) (ii)

safety[114]

5. Conformity assessment: All 'providers' intending to make available a high risk AI system in the market are required to undertake a conformity assessment. Everytime there is a change in the AI system which may affect its compliance with the regulations, a new conformity assessment is required to be undertaken.[115]
6. Database: The regulatory framework proposes that all high risk AI applications be registered in a common database. [116]
7. Human oversight: Human oversight is ensured through either one or all of the following measures:
   a) identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service;[117]
   b) identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user [118]
8. Risk assessment levels: 4 levels are risk are prescribed -
   a) Minimal risk
   b) Limited risk
   c) High risk
   d) Unacceptable risk: For AI applications with unacceptable risk, a complete or partial ban is proposed.

(IV) Common Features of Risk Management Frameworks and their role in mitigating risks posed by AI: Upon perusal of the three risk management frameworks discussed hereinabove, certain common features are evident:

1. Risk assessment levels: AI applications are classified as per the risk that they may pose to concerns such as privacy, security, bias etc. For each category of risk, certain measures are proposed - the severity of which increases from minimal restrictions to outright bans.
2. Transparent and Explainable AI: Transparent and Explainable AI have been ensured by making provisions for open source code and obliging concerned entities to explain the decision-making process of the AI. This is to counter the problem of opacity / black-box algorithms.
3. Human oversight / intervention: Recognizing that it is not possible to entirely reply upon automated decision making systems owing to their susceptibility to manipulation (for example, in the form of data poisoning or use of adversarial inputs), risk management frameworks have included human oversight / intervention to eliminate or mitigate the risk posed by AI.
4. Obliging concerned entities to ensure quality data.
5. Auditing of AI systems

(C) Areas where regulatory interventions are required: It is evident from the perusal

[114] Artificial Intelligence (AI) Act proposal, Art. 13.3 (b) (iii)
[115] Artificial Intelligence (AI) Act proposal, Art. 19
[116] Artificial Intelligence (AI) Act proposal, Art. 60
[117] Artificial Intelligence (AI) Act proposal, Art. 14.3 (a)
[118] Artificial Intelligence (AI) Act proposal, Art. 14.3 (b)

of risk management frameworks that the areas where the regulatory interventions are required are high risk AI applications. For example, the proposed Artificial Intelligence Act of the European Union aims to heavily regulate the following high risk AI applications:

1. critical infrastructures (e.g. transport), that could put the life and health of citizens at risk;
2. educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams);
3. safety components of products (e.g. AI application in robot-assisted surgery); employment, management of workers and access to self-employment (e.g. CV-sorting software for recruitment procedures);
4. essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan);
5. law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence);
6. migration, asylum and border control management (e.g. verification of authenticity of travel documents);
7. administration of justice and democratic processes (e.g. applying the law to a concrete set of facts).[119]

Upon perusal of the example discussed hereinabove, it is clear that the aforesaid high risk AI technologies may directly impinge upon privacy, security and may promote bias. Hence, regulatory interventions are required to mitigate the risk by ensuring quality training data,logging to ensure traceability of data, appropriate levels of human intervention, robustness and security etc.

(D) Implementation of measures in the context of NETRA: In the proposed NETRA Model, a Compliance Assistance Cell is envisaged to be created. It is recommended that NETRA, through its Compliance Assistance Cell, may prescribe:

1. Best organizational practices for organisations involved in the development of high risk AI applications;
2. Risk management framework, which includes ensuring compliance with transparency, explainability, bias mitigation and quality data assurance obligations - and upon non-compliance, enact penalizing measures including outright bans on extreme risk AI applications;
3. Conformity assessments to ensure compliance with risk mitigation measures and AI ethical principles;
4. A publicly available Algorithmic Impact Assessment tool created by NETRA for the benefit of the developers.
5. Assisting organizations to develop fairness toolkits to counter the risk of bias in AI
6. Creating and updating a database of high risk and extreme risk AI applications

It is further envisaged that the Compliance Officers of NETRA's Compliance Assistance Cell (who are the direct point of contact between the regulator and the developer), be entrusted with the responsibility to undertake conformity assessments and to ensure general compliance with the aforementioned.

Question 19 (b): Which are the potential technologies likely to be available in the near future to

[119] European Commission, *Regulatory framework proposal on artificial intelligence* (2021) Available at Regulatory framework proposal on artificial intelligence | Shaping Europe's digital future (europa.eu) (Last visited September 15, 2022)

further strengthen privacy?

EU's strategy - https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

When the privacy policy is unreadable
A proposed solution for the unreadable (and therefore unread) privacy policies was P3P. With this technology, a software user agent would read the privacy policy for the user, compare that policy with the user's privacy preferences (as captured in a file stored on the user's machine), and alert the user only if a mismatch was detected. In this way, the user did not need to read any privacy policies, but the privacy policy of every single visited website (in fact, every web page of every website) would be carefully read by the user agent. In order to make this work, standardized syntax and semantics for privacy policies was needed, which is precisely what the P3P Recommendation specified.

XACML

XACML defines standardized syntax and semantics for writing access control policies, along with the necessary decision request & response messages that allow a PDP to determine whether an access request should be granted or denied. Simple examples of XACML policies are presented in section results of XACML (2017). We also created our own very simple XACML policy which was used to produce a valid P3P policy; please see Appendix A for details.
Note that a recent paper by Jiang and Bouabdallah (2017) proposed JACPoL as an alternative to XACML that is based on JavaScript Object Notation (JSON) instead of XML and is therefore simpler and more efficient, while retaining descriptive power and human-readability. Although we explored JACPoL to some extent, for our proof-of-concept implementation we used XACML due to the availability of XSLT and the fact that both XACML and P3P are written in XML.

P3P

A P3P policy states the privacy practices of the website in a standardized format so that it can be read by a software user agent. It includes information about what data is collected, how long it is stored, who it may be shared with, and who a user should contact in the case of any disputes. A simple example of a P3P policy is presented as Example 3.2 in P3P (2002).
For our implementation, we created several simple P3P policies representing different privacy practices. This allowed us to easily test different scenarios (e.g., the P3P policy perfectly matched the user's preferences, or it did not match for any of several defined reasons). We also derived a very simple P3P policy in an automated way from our XACML policy; please see Appendix B for details.

XSLT

XSLT is a mechanism that can be used to transform an XML document into another XML document in a fully automated way. An XSLT Stylesheet is used to specify the transformation rules to be applied to the source document in order to transform it into the resulting document (note that the stylesheet itself is also written as an XML document). An XSLT Processor then inputs the source document and the stylesheet and outputs the resulting document. Finally, an

XSLT Formatter can be used to pretty-print the resulting document for display purposes, if desired.

Addressing Questions on Regulatory Sandboxes and Lighthouse Projects

Experimental Technologies - Data Protection and AI in Telecommunications

Questions 25, 27, 28, 29

<u>Question 25:</u> **Whether there is a need to create AI-specific infrastructure for the purpose of startups and enterprises in the telecom sector to develop and run AI models in an optimised manner? Whether such an infrastructure should cover various real-world scenarios such as cloud AI, edge AI and on-device AI? Please justify your response with rationale and suitable examples, if any.**

Yes, there is a need to create an AI-specific infrastructure in the telecom sector to develop and run AI models in an optimised manner. Such an exercise is also referred to as a 'regulatory sandbox' which should include real world scenarios. Regulatory sandboxes have proved to be beneficial in other sectors in India and have been successfully performed before. A 'sandbox' derived from a children's playground feature,[120] refers to a safe or controlled environment where new technology can be tested against a regulatory framework. The results of the sandbox are then used to create and implement a regulatory framework which would apply to the open market. It increases information sharing and communication between enterprises and startups (*hereinafter referred to as "innovators")* and the regulator. The Indian experience has primarily been focused in regulatory sandboxes in the fintech sector.[121] Recent sandboxes include: Ayushman Bharat Digital Mission (ABDM) sandbox,[122] the ABHA number service[123] in the health sector, Ministry of Housing and Urban Affairs' U-box, done for smart cities, digital technologies and urban development,[124] etc. The Telecom Commercial Communications Customer Preference Regulations, published by TRAI in 2018 also provided for regulatory sandboxes for DLT networks and auto callers/ robo calls, this would allow such functions or networks to operate in

[120] Cristina Poncibo and Laura Zoboli, Sandboxes and Consumer Protection: The European Perspective 2 International Journal on Consumer Law and Practice Vol 8 (2020).

[121] Shashidhar K,J,, Regulatory Sandboxes: Decoding India's attempt to Regulate Fintech Disruption, Observer Research Foundation (May 20, 2020), available at https://www.orfonline.org/research/regulatory-sandboxes-decoding-indias-attempt-to-regulate-fintech-disruption-6642. See Department of Banking Regulation, Reserve Bank of India, *Enabling Framework for Regulatory Sandbox*, available at https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/ENABLING79D8EBD31FED47A0BE21158C337123BF.PDF

[122] National Health Authority, *Sandbox Request Form*, available at https://sandbox.abdm.gov.in/applications/Integrators.

[123] National Health Authority, *ABHA Number Service*, available at https://sandbox.abdm.gov.in/docs/healthid.

[124] National Institute of Urban Affairs, *Sandbox,* available at https://nudm.mohua.gov.in/sandbox/.

controlled markets and the regulator could introduce new regulatory compliances which could cost innovators lesser. [125]

Globally, regulatory sandboxes have been in use since 2016 when the UK Financial Conduit Authority (FCA) launched the FinTech sandbox. Information and Communication specific sandboxes have been conducted in several latin american countries[126] such as Colombia[127] and an AI & Data Protection sandbox has been conducted by the Norwegian Data Protection Authority.[128]

In our opinion, a sector-specific approach is counterproductive to the objective of regulatory sandboxes. The aim of a regulatory sandbox is not to promote growth in one sector, there are other policies and mechanisms to ensure sector-specific growth. Thus, instead of a sector-specific approach, a technology-specific approach is warranted.[129] The aim of a regulatory sandbox is not to promote growth in certain sectors, but to develop technology.

Every regulator shall develop its own technology. Since AI is a combination of multiple technologies[130], it shall be the responsibility of NETRA to oversee the development of all technologies to ensure that innovation is not limited to a certain sector. This is also an incentive to innovators, since innovation in any technology would make their technology more efficient and modern, compared to different sectors being walled off.[131]

<u>Question 27:</u> Whether there is a need to establish experimental campuses where startups, innovators, and researchers can develop or demonstrate technological capabilities, innovative business and operational models? Whether participation of users at the time of design and development is also required for enhancing the chances of success of products or solutions? Whether such a setup will reduce the burden on developers and

[125] Telecom Commercial Communications Customer Preference Regulations, 2018, available at https://trai.gov.in/sites/default/files/RegulationUcc19072018.pdf.

[126] BNAmericas, *What to expect from regulatory ICT sandboxes in 2022,* Dec 29, 2021, available at https://www.bnamericas.com/en/features/what-to-expect-from-regulatory-ict-sandboxes-in-2022.

[127] Digital Regulation PLatform, *Case Study: Regulatory Sandbox Framework in Colombia*, Feb 24, 2021, available at https://digitalregulation.org/case-study-regulatory-sandbox-framework-in-colombia/.

[128] Birgitte Kofod Olsen, *Sandbox For Responsible Artificial Intelligence*, DATA ETHICS, Dec 14, 2020, available at https://dataethics.eu/sandbox-for-responsible-artificial-intelligence/.

[129] Manohar Samal & Puolomi Chatterjee, Regulatory Sandboxes for Artificial Intelligence: Techno-legal Approaches for India 33 (2009).

[130] Amber Sinha, Elonnai Hickok and Udbhav Tiwari, Response Submission on TRAI's Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector, 2017.

[131] *Supra* note 1.

enable them to focus on their core competence areas? Please justify your response with rationale and suitable examples, if any.

Yes, we do require the establishment of experimental campuses to innovate in AI technology. The lighthouse project business model is a model first used in manufacturing to set up some leading manufacturing hubs with world-class technologies that would serve as 'beacons' to the rest of the world.[132] Lighthouse projects are meant to promote innovation, they are allowed to test and use processes separate from the regular manufacturing of the company, so as to not disrupt their supply chain and to also find a way to increase their efficiency.[133]

We support the lighthouse project model to promote AI innovation. A lighthouse project in the field of AI is expected to incentivise the AI community to collaborate on key AI research challenges rather than working in silos, which leads to wasted efforts. Some of the benefits of a lighthouse project are listed under:

1. **Open innovation and collaboration** — Lighthouses involve collaboration from universities, startups, and other technology providers, ensuring that no one player or industry benefits disproportionately from innovation, and that everyone is given a chance to innovate.[134]
2. **Large and small companies** —The open collaboration and innovation mentioned above makes it possible for a small or medium-sized company to test out their products by securing funding from elsewhere. The pro-collaboration aspect of Lighthouses make it a natural fit for small and medium firms.

Other benefits include a level playing field for both emerging and developing economies[135], and democratised technology.

Some lighthouse projects that have been initiated in India include the 'Model Housing Projects for cost-effective, environment friendly and speedier construction'[136] launched by the Ministry of Housing and Urban Affairs, wherein the Union has set up Affordable Sustainable Housing Accelerators – India Centres to promote affordable housing.

[132] World Economic Forum, *These 10 new 'Lighthouse' factories show the future of manufacturing is here*, Sep 17 2020, available at https://www.weforum.org/agenda/2020/09/manufacturing-lighthouse-factories-innovation-4ir/.
[133] MCKINSEY GROUP, *'Lighthouse' manufacturers lead the way—can the rest of the world keep up?* 5 (January 2019).
[134] *Id.* at 6.
[135] *Id.*
[136] Press Release, MINISTRY OF HOUSING AND URBAN AFFAIRS, March 14, 2022, available at https://static.pib.gov.in/WriteReadData/specificdocs/documents/2022/mar/doc202231424601.pdf.

Looking abroad, we can see that India does have the ability to establish leading lighthouse projects. The Tata Steel, Steel Products Manufacturing Plant in the Netherlands is an example of such a facility.[137] It serves as living proof that India can, using a PPP model, establish such centres as well. Lighthouse projects, specifically 'Lighthouse campuses' will bring together stakeholders from research, innovation and deployment, to become a world reference in AI that can attract investments and the best talents in the field.[138] These campuses will build on key pillars, each of them being a network of excellence centres specialising in a given topic. Furthermore, NETRA shall be the parent regulator for these campuses, but will do little actual regulation to let innovation flourish. An IIT-like model is envisaged for such campuses.

Question 28: Whether experiments are required to be backed by regulatory provisions such as regulatory sandbox to protect experimenters from any violation of existing regulations? Whether participation of government entities or authorities during experimentation will help them to learn and identify changes required in the existing regulations or introducing new regulations? Please justify your response with rationale and suitable examples, if any.

Private sandboxes are spaces that are set up by the industry itself, where the innovators are free to test their technologies without entering the real-time market.[139] A private sandbox is, unlike a regulatory sandbox, not exempt from certain regulations imposed in the real world. If the private sandbox is to remain like this, then it does not need regulatory oversight, since it is already liable to follow all laws and regulations.

It becomes more interesting when private sandboxes get exemptions from following certain regulations. Private sandboxes are most likely to be created by innovators who were not authorised to participate in the regulatory sandbox.[140] Since these companies are those who had consented to be bound by the terms of the regulator anyway, and who were rejected from authorization for presumably good reason, it is necessary for the regulator to regulate them. Since our main model is technology-specific, and these private sandboxes are set up by industry -

[137] MCKINSEY GROUP, *'Lighthouse' manufacturers lead the way—can the rest of the world keep up?* 4 (January 2019).

[138] Euro Access (Macro Regions), Call: European Network of AI Excellence Centres: Pillars of the European AI Lighthouse, available at https://www.euro-access.eu/calls/european_coordination_awareness_standardisation__adoption_of_trustworthy_european_ai_data_and_robotics_ai_data_and_robotics_partnership_csa.

[139] FINANCIAL CONDUCT AUTHORITY (UK), *Regulatory Sandbox*, 12 (2015).

[140] *Id.*

thereby adopting a sector specific approach - the regulators are not fit to handle them. Either a separate sub-wing must be constituted under NETRA just for private sandboxes, or NETRA itself directly oversees them. The former appears to be a better answer than the latter.

Another concept we may consider is a sandbox umbrella. It is a non-profit company created for unauthorized innovators to test their technology solutions.[141] The umbrella company shall act as the representatives of all firms concerned here and be authorized by the regulatory authority even if the firms are by themselves unauthorized.

In our opinion, private sandboxes should be allowed. If the exemptions they get from liability are none to very little, then there is not much of a need to regulate them especially. If they get exemptions, then they must be regulated with great scrutiny. Under a sandbox umbrella, the regulatory authority should help every industry set up an umbrella company if it wants to.

Issue of Ownership: There are also questions regarding the ownership of the sandbox platform, or more accurately, the structure of the ownership of the platform, as to whether it is solely owned and operated by a Governmental organisation/regulator, whether it is a joint venture or if it is to be run wholly by a private entity, or a special purpose vehicle created for this purpose. We recommend that having it run wholly by the government, but funded by a PPP Model would increase accountability. Ideally, the State would both fund and regulate these spaces, so that innovators can consolidate capital only towards testing, but the State has limited resources. In a PPP Model, the chain of command is clarified, since there is only one authority to report to, and funds are arranged.

However, a state regulatory sandbox would help identify the existing lacunae in current telecom laws, which have been observed to have less regulations on private companies, service providers, especially when it comes to consumer data protection. [142] Thus, since the level of data protection in existing telecommunication laws is insufficient, testing AI technologies in the backdrop of proposed regulations would be beneficial and provide for empirical evidence while making the new Data Protection Bill, which was rolled back by the govt. The telecom sector laws we would need to consider include:

[141] *Id.* at 13.

[142] Rahul Matthan, Manasa Venkataraman and Ajay Patri, Privacy, Security and Ownership of Data in the Telecom Sector, *I*n response to comments sought by the Telecom Regulatory Authority of India, Takshila, (October 2017), available at https://trai.gov.in/sites/default/files/Takshashila_07_11_2017.pdf.

1) The Telecom Regulatory Authority of India Act, 1997;
2) The Information Technology Act, 2000
3) The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
4) The Telecom Commercial Communications Customer Preferences Regulations, 2018

These rules are not regulatory sandbox-specific (except the 4th one), but they relate most closely to any legislation governing the use of AI in a regulatory sandbox. Only the Telecom Commercial Communications Customer Preferences Regulations, 2018 acknowledges the existence of regulatory sandboxes. NETRA, a statutory body, will have to incorporate these standards in addition to its regulatory framework.

Other Global regulatory standards that NETRA should incorporate can be seen from "Responsible AI for All" published by NITI Aayog, which lays down principles to ensure that AI causes no harm which are:

- the principle of safety and reliability;
- the principle of equality;
- the principle of inclusivity and non-discrimination;
- the principle of privacy and security;
- the principle of transparency;
- the principle of accountability; and
- the principle of protection and reinforcement of positive human values.[143]

Accountability can be ensured, or at least bolstered, by setting the terms of ownership of such a sandbox platform correctly.

Some other accountability measures may include:

- Competent Judicial Authority: Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

1. separate and independent from the authorities conducting Communications Surveillance;
2. conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights; and
3. have adequate resources in exercising the functions assigned to them.[144]

[143] NITI Aayog, *Responsible AI for All Part I: Principles for Responsible AI,* 18, available at https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf (Last Visited on Feb 2021).

<u>Question 29:</u> In response to Q.27 and Q.28, whether establishing such a campus under government patronage will enable easy accessibility of public resources such as spectrum, numbering and other resources to the researchers? Whether it would be in mutual interest of established private players as well as startups, innovators and enterprises to participate in such experiments? Please justify your response with rationale and suitable examples, if any.

Balancing interests of innovators and enterprises

Innovators stand to gain large benefits by participating in a regulatory sandbox. Firstly, they can test out new products, services, features or technologies, without having to pass all stages of govt. sanction such as licensing etc. since it is only in a testing stage, secondly, they are able to test it against a regulatory framework- which, when implemented, they help to mold. Thus, there is increased communication between innovators and regulators, neither of the sides need to operate individually and the ultimate regulation is a product of collaborative effort. Hence, participation in the regulatory sandbox is of mutual interest of telecom innovators and the regulator. In some scenarios, it has been observed that less restrictive regulatory frameworks encourage an increased participation of innovators. [145] In case the regulatory framework is too strict or does not protect the innovators/enterprises interests, the sandbox may fail as it might not attract the desired participants. Thus, we recommend the following measures to balance the interests of innovators with the regulation:

a. **Periodic Review Process:** In order to realise communication between innovators and the regulator, it is necessary to have periodic reviews. We recommend that such a review takes place every six months until the sandbox is completed. The innovators should each submit a report, detailing what aspects of the framework are working well and which ones are not, which should be submitted to be reviewed by the regulator's two-tier panel.
b. **Liability Exemptions:** Previously, most Indian Sandboxes have not provided for any legal waivers.[146] In case of consumer grievances during the sandbox the innovators shall be liable, since providing an exemption cannot be replicated once in an open market.

[144] Amber Sinha, Elonnai Hickok and Udbhav Tiwari, Response Submission on TRAI's Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector, 2017.

[145] Sophie Quinton, 'Relaxed Rules Attract Entrepreneurs to State 'Sandboxes' PEW (June 15, 2021), available at https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/06/15/relaxed-rules-attract-entrepreneurs-to-state-sandboxes.

[146] Reserve Bank of India, Enabling Regulatory Sandboxes,, 4.1. (August 13, 2019), available at https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=938#4.

Giving exemptions would destroy the representative value of the sandbox. Instead, innovators can include in their proposals (before being accepted to participate) their policy and mechanism for grievance redressal, in order to limit their liability to some extent. Previously, in FinTech sandboxes the RBI had compulsorily required companies to take insurance prior to participating in the sandbox. This insurance was for consumer compensation which may be required for any grievances caused during the sandbox. In no way shall the sandbox serve a purpose to bypass existing legislation.[147] The draft AI Act prepared by the European Commission also does not provide for liability exemption during sandboxes.[148]

c. **Revealing Trade Secrets:** Some authors suggest that sandboxes facilitate the exchange of information along with facilitating exposing algorithmic codes and trade secrets of innovators to their market competitors, which discourages their participation.[149] To tackle this issue the innovator will have to play a careful role in balancing the interests of innovators i.e. protecting their trade secrets and facilitating information exchange between the participants to aid innovation.

Protecting Consumer Interests & Rights during in the Regulatory Sandbox

A regulatory sandbox offers benefits to all consumers. By offering the chance to test out advanced technologies such as AI, it creates opportunities to develop better services and encourages participation of new enterprises. This ensures a wider market choice for consumers.[150] In addition to this, a regulatory sandbox tests out a set of regulations on a limited market, in absence of this un-tested rules would be imposed on an open market, where public consumers would be affected all at once. However, consumer rights should not be harmed while focusing on innovator regulation. Hence, to protect the rights of consumers we recommend that:

[147] Poornima Advani, 'Regulating to Escape Regulation: The Sandbox Approach' Mondaq (January 11, 2021), available at https://www.mondaq.com/india/fin-tech/1023942/regulating-to-escape-regulation-the-sandbox-approach

[148] Tambiama Madiega with Anne Louise Van De Pol, Artificial Intelligence act and regulatory sandboxes, European Parliamentary Research Service (June 2022), available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf

[149] Jon Truby, A Sandbox Approach to Regulating High-Risk Artificial Intelligence Application, European Journal of Risk Regulation (2022), 13, 270–294.

[150] Cristina Poncibo and Laura Zoboli, Sandboxes and Consumer Protection: 8 The European Perspective 2 International Journal on Consumer Law and Practice 16 (2020).

a. **Restricting types of consumers:** Since a telecommunication AI sandbox has not been performed in India before, we recommend that the first regulatory sandbox or phase I is *not* an open market operation as the pan India telecommunication market would be too wide. Alternatively, we recommend that phase I consumers should be private consumers such as institutions, other businesses etc.[151] who would be more equipped and digitally literate to participate in such an operation. Public or retail consumers should not be allowed to participate. This would ensure that risks and consumer rights violations are mitigated. In case consent is sought from individual consumers, the conditions imposed may be too burdensome as some consumers may not be able to deny use of an essential telecommunication service. Testing should also be limited to consumers of a local/regional market. [152]

b. **Transparency and consent:** We recommend that consumers are informed about their participation in a regulatory sandbox.[153] Both new and existing consumers should be notified that certain features of their service or the entire service will be a part of a telecommunication regulatory sandbox, such a notification should explicitly state the AI technologies that will be tested and disclose how their personal information may be affected by it. The innovator must seek explicit consent for the same and re-notify in case of changes to the regulatory framework (for example: Phase II of the regulatory sandbox.) The sub-consumer i.e. the public consumer of the private consumer (i.e. even an employee/student/public consumer etc.) should also be notified and their participation needs to be consented.

c. Grievance Redressal Mechanism: Since consumers are private/institutions and innovators participating, have agreed to comply with a regulator, consumer complaints and grievances should be raised with the regulator itself. In case complaints are required to be sent to the innovators (which still can be sent) it may discourage smaller innovators from participating, who may not have the bandwidth to tackle the complaints. In case consumer classes are aggrieved or not satisfied with the remedies offered, the National Consumer Disputes Redressal Commission (or its appropriate state commission) or civil

[151] Point 2.3, Consumer Protection in Regulatory Sanboxes, Banking Stakeholder Group, Regulatory Sandboxes: A Proposal to EBA by the Banking Stakeholders group, July 20, 2017, available at https://www.eba.europa.eu/sites/default/documents/files/documents/10180/807776/dc1d5046-e211-4b24-aadf-33fc93949017/BSG%20Paper%20on%20Regulatory%20Sandboxes_20%20July%202017.pdf?retry=1.

[152] Cristina Poncibo and Laura Zoboli, Sandboxes and Consumer Protection: The European Perspective 2 8 International Journal on Consumer Law and Practice 5 (2020).

[153] Point 2.3, Consumer Protection in Regulatory Sanboxes, Banking Stakeholder Group, Regulatory Sandboxes: A Proposal to EBA by the Banking Stakeholders group, July 20, 2017 available at https://www.eba.europa.eu/sites/default/documents/files/documents/10180/807776/dc1d5046-e211-4b24-aadf-33fc93949017/BSG%20Paper%20on%20Regulatory%20Sandboxes_20%20July%202017.pdf?retry=1.

courts should have jurisdiction. Innovators should include in their proposal for the sandbox a provision for compensation/redressal.[154]

We do *not* recommend making consumers a third wing to the regulatory framework i.e. in addition to the regulator and innovators, but instead recommend that 'consumer representatives' are included in the regulator panel itself.[155] Such a representative could be brought in from consumer groups. It has been argued that making a tri-party sandbox often makes the operation more complex and is generally avoided by most regulatory sandboxes which have opted for a two-tier system.[156] International bodies, academics could also be represented, from whom the regulatory panel would seek advice from.

[154] Cristina Poncibo and Laura Zoboli, Sandboxes and Consumer Protection: The European Perspective 2 8 International Journal on Consumer Law and Practice 8 (2020).

[155] Point 2.3, Consumer Protection in Regulatory Sanboxes, Banking Stakeholder Group, Regulatory Sandboxes: A Proposal to EBA by the Banking Stakeholders group, July 20, 2017, available at https://www.eba.europa.eu/sites/default/documents/files/documents/10180/807776/dc1d5046-e211-4b24-aadf-33fc93949017/BSG%20Paper%20on%20Regulatory%20Sandboxes_20%20July%202017.pdf?retry=1

[156] Walter G. Johnson, *Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies,* REGULATION & GOVERNANCE, available at https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12487

ADDRESSING QUESTIONS ON ACADEMIA AND INDUSTRIAL LINKAGES

Questions 34, 38, and 39

<u>Question 34:</u> Whether the courses or programs related to AI/ML currently being offered by various institutions and universities in India are adequate to meet the capacity and competence required to develop and deploy AI solutions or products in the telecom networks? If not, what additional steps or measures are suggested to fill the gap? Please justify your response with rationale and suitable examples, if any.

We explored the details publicly available on the official websites of IITs, NITs, IIITs, IISc Bangalore and Bits Pilani in India. The details may be found in "Annexure C".

After going through the curriculum of different AI courses offered across manifold universities in India, the researchers have identified the following lacunas and proposed the following suggestions:

1. No uniformity in the courses offered/ no structure: There is no coherence in the AI and machine learning curriculums followed by various universities. This creates a barrier to incorporating AI into mainstream education. People want to do it for extra credit rather than to build a career in the field. A clear syllabus at the undergraduate level will inspire students to pursue AI in its entirety rather than as an extra credit course. It is critical to ensure that any institution's program credentials include a well-structured curriculum that is jam-packed with industry-relevant case studies and projects, mentored sessions, and enough handholding to achieve a thorough understanding of the concepts.

2. Apprehensions regarding AI: People frequently have reservations due to a lack of awareness. The fact that a particular specialisation is in high demand does not imply that universities will develop a Btech course in that field. Universities believe that the courses offered in the final year of Btech programmes are adequate for learning AI. Furthermore, it is anticipated that career opportunities for AI graduates will be limited. As a result, a Btech in computer science and electrical engineering with a few AI courses is thought to provide far more options than a Btech in AI. Before enrolling in a programme, factors such as accessibility, flexibility, career support, curriculum, and industry relevance are always considered, whether it is a B Tech in AI or any other AI programme available.

3. Lack of trained faculty: Currently, every educational institution recognises the importance of instilling in their students career-critical competencies. The main issue is a scarcity of trained faculty in new-age skills. To provide world-class education in fields such as AI, analytics, machine learning, and cloud computing, hiring new teachers or upskilling existing ones becomes critical.

4. The need for the intersection of AI and other social sciences: All departments of social sciences will be required to teach basic AI as well as some advanced topics that will vary by department. Humanities do not currently require AI, but this may change in the near future. Colby College, a liberal arts college in Waterville, Maine (USA), for example, has integrated AI into nearly every discipline, from computer science to English literature, in addition to specialised degree programmes and AI research. Another example is Carnegie Mellon University, a leading university in Pittsburgh, Pennsylvania (USA), which has integrated AI and technology instruction throughout its entire MBA programme. It is also one of the world's leading artificial intelligence education and research centres.

5. Lack of state funding: There aren't enough central initiatives to support the implementation and spread of AI in universities. AI cannot thrive without the government's support and commitment. The French government has stated that it will invest €1.5 billion ($1.85 billion) in artificial intelligence research until 2022. Following the British government's recommendations in late 2017, the autumn budget promised new funds, including at least £75 million for AI. Similarly, the Canadian government developed a $125 million "pan-Canadian AI strategy" last year.

6. Develop contextual standard benchmarks to assess quality of algorithms: Standard benchmarks can aid in assessing the quality and appropriateness of algorithms, in part due to the urgency of AI development and implementation in enabling effective assessments of algorithms to understand impact and informing selection by institutions adopting solutions. Such benchmarks may be most effectively defined at a sectoral level (finance, for example) or by technology and solution (facial recognition etc.). Ideally, the government would lead these efforts in collaboration with multiple stakeholders.

7. Coordination and collaboration across stakeholders: Contextually Nuanced and Appropriate AI Solution Development It is critical that solutions used in India account for cultural nuances and diversity in order to ensure effectiveness and accuracy. According to our findings, this could be accomplished in a variety of ways, including training AI solutions used in health on data from

Indian patients to account for demographic differences[42], focusing on natural language voice recognition to account for the diversity of languages and digital skills in the Indian context, and developing and applying AI to reflect societal norms and understandings.

8. Focus on marginalized groups: National minorities, including rural communities, the disabled, and women, should be targeted for increased awareness, skills, and education. Furthermore, there should be a concerted focus on under-represented communities in the tech sector, such as women and sexual minorities, to ensure that the algorithms and the community working on AI-powered solutions are holistic and cohesive. Iridescent, for example, focuses on girls, children, and families to help them adapt to changes such as artificial intelligence by encouraging curiosity, creativity, and perseverance in order to become lifelong learners. This will be critical in ensuring that AI does not exacerbate societal and global inequalities, including digital divides. Widespread use of AI will undoubtedly necessitate re-skilling various stakeholders in order to raise their awareness of AI's potential. Artificial intelligence can be used as a resource in the re-skilling process, just as it is used in the education sector to assess people's comfort with technology and fill gaps.

9. Early Childhood Awareness and Education: It is critical that AI awareness begins in early childhood. This is due in part to the fact that children already interact with AI and will continue to do so in the future, necessitating an understanding of how AI works and how it can be used safely and ethically. It is also critical to begin developing the skills that will be required in an AI-driven society at a young age. A government report on artificial intelligence and emerging technologies in schools that discusses the need for AI from the ground up and the smooth implementation of AI.

10. Skill sets to successfully adopt AI: Educational institutions should provide opportunities for students to learn how to adapt to the adoption of AI, as well as push for academic programs centered on AI. It is also critical to incorporate computing technologies such as AI into medical schools in order to prepare doctors for the technical skill sets and ethics required to integrate AI into their practices. Similarly, IT institutes could include courses on ethics, privacy, and accountability, among other topics, to help engineers and developers understand the issues surrounding the technology and services they are developing.

We analyzed the curriculum of universities across the globe that can act as a reference model for developing successful AI models in India.

<u>Questions 38 and 39:</u> Whether there is a need to establish telecom industry-academia linkages specifically for AI and BD to accelerate the development and deployment of AI products and solutions? Whether there is a need to establish Centres of Excellence (CoEs) for this purpose or it can be achieved by enhancing the role of existing TCoE? Please justify your response with rationale and global best practices, if any. And Whether there is a need to establish telecom industry-academia linkages specifically for AI and BD for AI related skill development? Please give the suggestions for strengthening the industry-academia linkages for identification of the skill development courses. Please justify your response with rationale and global best practices, if any.

Center of Excellences: The way forward

Most of the universities in India are not like the universities which have been considered while looking at the courses for AI and BD. Foreign universities offer a multitude of courses. While most Indian universities are focused on one aspect of education. IITs, NITs focus on engineering while IIMs focus on management studies. There are research tie ups between universities however, these tie ups are mostly limited to certain projects. To push for development of Indian academia and industry it is imperative that any center of excellence is able to address all three aspects of the field: technological, managerial and legal.

Looking towards the West

Universities such as Harvard, Stanford, Oxford among others offer a multitude of courses. These universities offer an education in all the three aspects. Thus, the Centers of Excellences they have are a much more holistic approach towards the research.
Berkman Klein Center, Harvard University's COE, offers a variety of courses. They not only offer courses which are targeted towards technology but also offer courses which talk about management and law such as Ethics and AI. The Center can thus pull from various experts who are able to nurture the growth of AI.

India needs to create such centres of which operate in an interdisciplinary manner. To make that possible it is necessary to create bridges between the various fields. Thus, a Center of Excellence means that there is an interdisciplinary focus on development on AI and BD.

However there are a few problems which arise when creating such centers.

If we look geographically it becomes difficult for such holistic centers to come up in India. Let us take Mumbai for example. It has an IIT and an NLU however, there is no IIM. Thus, the first barrier to formation of such centers becomes the geographical location.

The second issue which hinders the creation is that of the research which is conducted at the centers and the support provided by universities. Many institutes in India do not engage in critical research even at the highest level. There ano mechanisms for research in India nor does there exist a mechanism which talks about research universities. The collaboration would mean an equal or pre-determined pooling of resources to make sure that development happens in this field.

This is where the role of industry becomes important in the development of AI and BD. The industry can help bridge these gaps. The problem of funding is easily solved by the investment an industry can make into a COE. The funding by industry would also mean obligations on the COE to complete the research which the COE undertakes. The industry can ensure that the courses offered by the COEs are not only helping the academia but also tailored towards the needs of the industry.

There needs to be checks and balances in place to ensure that the funding by industry would not beholden COEs to the whims and fancies of the industry. While such a belief might be cynical, there exists a risk that the industry could treat the COE as personal R&D departments. The primary people in the COE would be students and researchers who would be interested in the wonders which lay in the unexplored areas of the field. It is important for advancements in the field that they are given the unbridled opportunity to study and explore the fields.

A simple method of achieving this would be through the CSR initiatives that the industries contribute towards. Diverting CSR towards these COEs would mean that the COEs continue to be funded while having no formal obligation to comply with the demands of the industry.

This can also be achieved by collaborations between the government and large companies to promote accessibility and encourage innovation through greater R&D spending. The Government of Karnataka, for instance, is collaborating with NASSCOM to set up a Centre of Excellence for Data Science and Artificial Intelligence (CoE-DS&AI) on a public-private partnership model to "accelerate the ecosystem in Karnataka by providing the impetus for the development of data science and artificial intelligence across the country." Similar centres could be incubated in hospitals and medical colleges in India. Principles of public funded research such as FOSS, open standards, and open data should be core to government initiatives to encourage research. The NITI Aayog report proposes a two-tier integrated approach toward accelerating research, but is currently silent on these principles

Therefore, as suggested by the NITI AAYOG Report, the government needs to set up 'centres of excellence'. Building upon the stakeholders identified in the NITI AAYOG Report, the centers of excellence should involve a wide range of experts including lawyers, political philosophers, software developers, sociologists and gender studies from diverse organizations including government, civil society,the private sector and research institutions to ensure the fair and efficient roll out of the technology.[35] An example is the Leverhulme Centre for the Future of Intelligence set up by the Leverhulme Foundation at the University of Cambridge[36] and the AI Now Institute at New York University (NYU)[37] These research centres bring together a wide range of experts from all over the globe.

ADDRESSING QUESTIONS ON AI AND BIG DATA IN TELECOMMUNICATION SECTOR

Questions 30 and 33

Question 30: Whether active participation in the international challenge programs such as ITU (International Telecommunication Union) AI/ ML 5G challenge will help India's telecom industry in adopting AI? Whether similar programs are also required to be launched at the national level? Whether such programs will help to curate problem statements or help in enabling, creating, training and deploying AI/ML models for Indian telecom networks? What steps or measures do you suggest to encourage active participation at international level and setting up of such programs at national level? Please justify your response with rationale and suitable examples, if any.

Requirement of more R&D

According to the findings from a recent Brookings Institution study,[157] India ranked among the top 10 nations in terms of technological advancement and financial support in artificial intelligence. While it fared well in the areas of investment and expenditure on AI made by the public, government initiatives, as well as private sectors and organisations, it was observed that

[157] Samar Fatima, Gregory S. Dawson, Kevin C. Desouza, and James S. Denford, *How companies are leveraging computing power to achieve their national artificial intelligence strategies,* January 12, 2022, available https://www.brookings.edu/blog/techtank/2022/01/12/how-countries-are-leveraging-computing-power-to-achieve-their-national-artificial-intelligence-strategies/#cancel, (Last visited on September 14, 2022).

there was a scope of improvement in commercial and research-oriented initiatives for India.[158] In 2019, the Ministry of Electronics and Information Technology (MeitY) had constituted four Committees to address the possible impact of AI on the economy and society and to come out with a policy framework on AI.[159] The reports published by the Committees had also emphasised upon the importance of a strong collaboration effort between the industry and academia in the AI ecosystem. A joint effort of industry which focuses on advancing solutions of commercial challenges and building skillforce when combined with academia which focuses on generating knowledge and imparting education to students could help in addressing the major challenges of the field. The report had highlighted that the data and computation power that modern day industry possesses cannot be matched in any shape or form by academia. However, the foundational principles of AI/ML/DL that academia brings to the table cannot be easily found elsewhere and is extremely valuable. [160]

It was highlighted that a major limitation in generating outputs in terms of research publications is due to resource constraints.[161] In this regard, it was highlighted by the Committee that there is a need to focus on training the current and next generation(s) in both the fundamentals and applied areas of AI. It suggested that a systematic approach should be taken where such training begins right from the middle school level where students are exposed to real-life examples like weather prediction, score prediction, etc. The training should also involve the students at all levels of education to work with open source ML tools.

How challenge programs by ITU help in research areas (specifically standardisation)?

One of the ways to achieve the above-stated objectives is to encourage active participation of students in the international challenge programs as organised by the ITU and other organisations to foster an environment of technological innovation and creativity among the youth. The ITU Challenge program offers its participants with curated problem statements covering wide range of issues along with a mix of real-world and simulated data. It also trains the teams by means of

[158]INDIAai, *India ranks in the top 10 global AI adopters, with immense potential to grow: Study*, January 25,2022, available https://indiaai.gov.in/news/india-ranks-in-the-top-10-global-ai-adopters-with-immense-potential-to-grow-study, (Last visited on September 13, 2022).

[159] Ministry of Electronics & Information Technology, Government of India, *Artificial Intelligence Committees Reports*, January 11, 2022, available https://www.meity.gov.in/artificial-intelligence-committees-reports, (Last visited on September 14, 2022).

[160] SHRI R CHANDRASHEKHAR COMMITTEE, *Report Of Committee – C On Mapping Technological Capabilities, Key Policy Enablers Required Across Sectors, Skilling And Re-Skilling, R&D*, (July, 2019).

[161] While India ranked 3rd in terms of high quality research publications in the field of AI, however, the research documents produced by India (12,135 documents) were significantly lower than its competitors USA (32,421 documents) and China (37, 918 documents) according to an analysis done by a research agency *Itihaasa.*
Jacob Koshy, *India ranks third in research on artificial intelligence*, January 18, 2019, available https://www.thehindu.com/sci-tech/science/india-ranks-third-in-research-on-artificial-intelligence/article26030596.ece, (Last visited on January 14, 2022).

technical webinars, mentoring and hands-on-sessions to help them enable, create, train and deploy ML models for communication networks. The solutions created by the participants are also tested on real data and real-world programs.[162] More importantly, their solutions are called for submission to the peer-reviewed ITU Journal which is then utilised in the research areas of standardisation carried on by the ITU.[163] This is of great significance in the Indian context as it provides a unique solution to the problem of dearth of research and development initiatives.

Bug bounty challenges as a method to encourage active participation

In October 2020, people on Twitter raised concerns that the saliency model that was used to crop images didn't serve all people equitably. Shortly thereafter, Twitter published its algorithmic bias assessment[164] which confirmed the model was not treating all people fairly. In May 2021, it began rolling out changes[165] to decrease reliance on ML-based image cropping since the decision to crop an image is best made by people. In August 2021, Twitter organised the first algorithmic bias bounty challenge and invited the ethical AI hacker community to identify additional bias and other potential harms within it.[166]

The bias bounty challenge helped uncover a wide range of issues in a short amount of time coming from a diverse group of participants. The winning submission[167] used a counterfactual approach to demonstrate that the model tends to encode stereotypical beauty standards, such as a preference for slimmer, younger, feminine, and lighter-skinned faces. The second place[168] submission confirmed the age bias found by the first place submission by showcasing how the algorithm rarely chooses people with white hair as the most salient person in a multi-face image and also studied spatial gaze bias in group photos with people with disabilities. The third place[169] submission analysed linguistic bias for English over Arabic script in memes. The most innovative

[162]AIforGood, AI/ML in 5G Challenge, available https://aiforgood.itu.int/about-ai-for-good/aiml-in-5g-challenge/, (Last visited on January 14, 2022).

[163] Special issue on AI/ML solutions in 5G and future networks, available https://www.itu.int/en/journal/j-fet/2021/005/Pages/default.aspx, (Last visited on January 14, 2022).

[164] Kyra Yee, Uthaipon Tantipongpipat, Shubhanshu Mishra, *Image cropping on twitter: Fairness metrics, their limitations, and the importance of representation, design, and agency*, 5 Proceedings of the ACM on Human-Computer Interaction CSCW2, 1-24, (October 18, 2021).

[165] Dantley Davis, *Centre- cropped images on Twitter*, March 10, 2021, available https://twitter.com/dantley/status/1390040111228723200?s=20, (Last visited on Septempber 14, 2022).

[166] Rumman Chowdhury & Jutta Williams, *Introducing Twitter's first algorithmic bias bounty challenge*, July 30, 2021, available https://blog.twitter.com/engineering/en_us/topics/insights/2021/algorithmic-bias-bounty-challenge, (Last visited on Septempber 14, 2022).

[167] Bogdan Kulynych, *How to Become More Salient? Surfacing Representation Biases of the Saliency Prediction Model*, August 12, 2021, available https://github.com/bogdan-kulynych/saliency_bias, (Last visited on September 14, 2022).

[168] Erick Mejia Uzeda, *HALT Saliency Algorithm Bias Evaluation of Group Photos*, August 09, 2021, available https://github.com/erickmu1/Twitter-Algorithmic-Bias, (Last visited on September 14, 2022).

[169] Roya Pakzad, *Gazing at the Mother Tongue: Analyzing Twitter's Image Cropping Algorithm on Bilingual Memes*, August 09, 2021, available https://github.com/royapakzad/image-crop-analysis, (Last visited on September 14, 2022).

prize was given to an entry that demonstrated that the model prefers emojis with lighter skin.[170] And the most generalizable submission was for an adversarial approach that proved that by adding a simple padding around an image, the cropping can be avoided.

The results of their findings confirmed that certain challenges can only be solved when diverse voices are able to contribute to the conversation around bias in AI.

Other bug bounty programs for identification of AI bias

In April 2020, researchers from Google Brain, Intel, Stanford Centre for AI Safety, University of Oxford, University of Cambridge as well as other top research labs in the U.S. and Europe joined forces to formulate a toolbox for turning AI ethics principles into practice. It has set several guidelines, including paying developers for finding bias in AI, akin to the bug bounties offered in security software.[171]

Within the sphere of bias and safety bounties, the paper identifies a major problem i.e. there is too little incentive, and no formal process, for individuals unaffiliated with a particular AI developer to seek out and report problems of AI bias and safety. As a result, broad-based scrutiny of AI systems for these properties is relatively rare. Recommending that AI developers should pilot bias and safety bounties for AI systems to strengthen incentives and processes for broad-based scrutiny of AI systems, the paper states "While efforts such as red teaming are focused on bringing internal resources to bear on identifying risks associated with AI systems, bounty programs give outside individuals a method for raising concerns about specific AI systems in a formalised way. Bounties provide one way to increase the amount of scrutiny applied to AI systems, increasing the likelihood of claims about those systems being verified or refuted."

There are a plethora of popular bug bounty programs for detecting AI bias.

- Logically's Bug Bounty Program[172] works with security professionals to protect the customer's from harmful networks and mobile applications.

[170] Vincenzo di Cicco, *Twitter Crop Emoji Bias*, August 08, 2021, available https://github.com/0xNaN/twitter-crop-bias, (Last visited on September 12, 2022).

[171] Miles Brundage et al., *Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims*, available https://arxiv.org/pdf/2004.07213.pdf (April, 2020).

[172] Logically, *Bug Bounty Program 2021*, available https://www.logically.ai/bug-bounty-program, (Last visited on September 09, 2022).

- The Mozilla Security Bug Bounty Program[173] is designed to enforce security research in Mozilla software and provide an incentive to those who help make the internet a safer place.
- The Community Reporting of Algorithmic System Harms (CRASH) project[174] brings key stakeholders together for discovery, scoping and iterative prototyping of tools. This is to enable more accountable and harmless AI systems.
- HackerOne, a "hacker-based" security testing platform hosts 'The Internet Bug Bounty'[175]. This program rewards hackers who manage to uncover security vulnerabilities in some of the most important softwares on the internet. The program, managed by a panel of volunteers selected from the security community, is sponsored by Facebook, GitHub, Microsoft, Hackerone and Ford Foundation.
- Crowdsourced security platform by Bugcrowd[176] combines analytics, automated security workflows, and human expertise to find and fix critical vulnerabilities. Bugcrowd announced Series D funding in April 2020 of $30 million. It has an expansive list of clients they have worked with, including Tesla, Atlassian, Fitbit, Square, and Mastercard. They review platforms for big tech giants and retail space like Amazon and eBay.

Learnings from bounty challenges for AI regulation

When building machine learning systems, it's nearly impossible to foresee all potential problems and ensure that a model will serve all groups of people equitably. But beyond that, when designing products that make automatic decisions, upholding the status quo often leads to reinforcing existing cultural and social biases. Direct feedback from the communities who are affected by algorithms helps companies design products to serve all people and communities. This is where challenge based programs can be helpful, by creating an opportunity for people who have historically done this sort of work for free, and incentivizing them to be both recognized and rewarded for their contributions.

[173] Mozilla, *Security Bug Bounty Program*, available https://www.mozilla.org/en-US/security/bug-bounty/, (Last visited on September 09, 2022).

[174] Algorithmic Justice League, *Community Reporting of Algorithmic System Harms (CRASH) Project*, available https://www.ajl.org/avbp, (Last visited on September 14, 2022).

[175] Hackerone, *The Internet Bug Bounty*, available https://hackerone.com/ibb?type=team, (Last visited on September 14, 2022).

[176] Bugcrowd, *Bug Bounty*, available https://www.bugcrowd.com/products/bug-bounty/, (Last visited on September 14, 2022).

In a blog post sharing learnings from its first algorithmic bias bounty challenge,[177] Twitter acknowledged that they noticed multiple submissions that recognized the impact bias in ML can have on groups beyond those addressed in our previous work, such as veterans, religious groups, people with disabilities, the elderly, and individuals who communicate in non-Western languages. Often, the conversation around bias in ML is focused on race and gender, leading to the exclusion of various other forms that bias can take. Research in fair machine learning has historically focused on Western and US-centric issues. Twitter acknowledges that they were particularly inspired to see multiple submissions that focused on problems related to the Global South.

Twitter's post also talks about how submissions from a wide array of participants, ranging from individuals, to universities, startups, and enterprise companies, were encouraged. Above all, using a community-led approach is necessary to build better algorithms because people's lived experiences make it possible for them to discover unintended consequences which companies wouldn't have otherwise been able to. A possible challenge that one might face while organising such programs is creating a grading rubric in order to judge participants' submissions, inspired by previous frameworks in privacy and security for assessing risk. The challenge here is coming up with a rubric that is concrete enough to grade and compare submissions, but broad enough to encompass a wide variety of harms and methodologies. Several approaches can be taken to deal with this challenge. Twitter's approach was to focus on issues that have historically received less attention in fair ML research, such as representational harms. In its bounty challenge, it assigned a different number of points to different types of harms. Another way can be by encouraging qualitative analyses, grading each submission by not only their code, but their assessment of why their approach and perspective was relevant.

Proposals and Suggestions

- An approach similar to ITU can be taken at the national level where educational institutions supported by governmental organisations and the private sector (which can provide financial support) launch challenge-based programs and the problem statements cover real-life implementational challenges of AI in various sectors such as healthcare, financial, telecom, legal, etc. The programs should encourage students from different

[177]Rumman Chowdhury & Jutta Williams, *Introducing Twitter's first algorithmic bias bounty challenge*, July 30, 2021, available https://blog.twitter.com/engineering/en_us/topics/insights/2021/algorithmic-bias-bounty-challenge, (Last visited on Septempber 14, 2022).

disciplines of engineering, medical science, management, law, etc. to collaborate as a team and bring more comprehensive and creative solutions/research ideas to the table.

- Another approach to such programs can also include state-level challenge programs where the problem statements can be based on the nuanced issues involving the implementation of AI technology in that particular state. Such programs can be organised by the collaboration of the respective state governments and educational institutions of the state.
- Adopting the ITU approach, the best solutions to these programs can be compiled by and published in the E-Tech Data Library of the regulating body NETRA which could be utilised in creation of public policies (and other things like setting benchmark principles for specific sectors, standardisation, etc.)
- In 2021, the New York city council passed a bill[178] that required providers of automated employment decision tools to recruiters in the city to have their underlying AI algorithms audited each year. If such legislations are passed in India, bounty programs could be a cost-effective and community-based method to help companies or small start ups find previously undetected security flaws in their software.

Question 33: Whether active participation in the international bootcamp programs such as MIT Bootcamps, Design Thinking Bootcamp by Stanford University etc. will help India's telecom industry workforce to find international developers community, navigate challenges and learn from experiences of others? Whether similar programs are also required to be launched at the national level? What steps or measures do you suggest to encourage active participation at the international level and setting up of such programs at the national level? Please justify your response with rationale and suitable examples, if any.

International collaborations in AI

In recent times, various international approaches have been taken to address the opportunities and challenges presented by AI and to tackle the practical application of the same. The Indian strategy focuses on advancing research while dealing with issues such as ethics, bias, and privacy related to AI. It also focuses on economic growth and increasing social inclusion. This is reflected in the fact that India stands at the 6th position on Stanford's Global AI Vibrancy ranking and aces the 'Inclusion' parameter.[179]

[178] Nathaniel Mott, *New York City Passes Bill to Address Bias in AI-Based Hiring Tools*, November 21, 2021, available https://www.pcmag.com/news/new-york-city-passes-bill-to-address-bias-in-ai-based-hiring-tools, (Last visited on September 14, 2022).

[179] Stanford's Institute for Human-Centred Artificial Intelligence, *Artificial Intelligence Index 2021 Annual Report,* (March, 2021), available at http://creativecommons.org/licenses/by-nd/4.0/ (last visited on September 14, 2022).

India has collaborated with Germany to work on AI focusing on healthcare and sustainability. The initiative is led by the Indo-German Science and Technology Centre (IGSTC) and is a joint initiative by the Department of Science & Technology (DST), GoI, and the Federal Ministry of Education and Research (BMBF), Government of Germany, to facilitate Indo-German research and development.[180]

India and U.S. launched the Indo-U.S. Science and Technology Forum's U.S. India Artificial Intelligence (USIAI) Initiative[181] to serve as a platform to discuss opportunities, challenges, and barriers for bilateral AI R&D collaboration, enable AI innovation, help share ideas for developing an AI workforce, and recommend modes and mechanisms for catalysing partnerships.

Furthermore, India joined the Global Partnership on Artificial Intelligence (GPAI),[182] a multi-stakeholder international project which uses the expertise and diversity of different participating countries to govern the responsible development and use of artificial intelligence (AI) based on human rights, inclusiveness, diversity, creativity, and economic prosperity.

Bootcamps as a method to encourage active participation

Boot camps are short-termed intense training sessions that are designed as a way to prepare learners for the practical reality of coding and programming. The demand for highly skilled technology professionals has led to the development of boot camps across the globe. Bootcamps help bridge the skill gap that industry demands from entry level techies and what colleges are able to do.

A plethora of AI bootcamps are being organised at the international level. The Private AI Bootcamp offered by Microsoft Research (MSR)[183] focuses on tutorials of building privacy-preserving machine learning services and applications with homomorphic encryption (HE). The program contents are specifically designed for training, where participants master the use of HE, the Microsoft SEAL library, and the methodology behind building privacy-preserving machine learning solutions. As a project as well as a competition, students work in teams, design and pitch a novel technology built upon what they have learnt during the bootcamp, and receive

[180] Federal Ministry of Education and Research, *Indo-German Science and Technology Centre (IGSTC),* available at https://www.internationales-buero.de/en/igstc.php, (Last visited on September 14, 2022).

[181] Department of Science & Technology, *US India Artificial Intelligence (USIAI) Initiative launched,* available at https://dst.gov.in/us-india-artificial-intelligence-usiai-initiative-launched, (Last visited on September 14, 2022).

[182] OECD.AI, *The Global Partnership on AI (GPAI),* available at https://oecd.ai/en/gpai, (Last visited on September 14, 2022).

[183] Microsoft, *Private AI Bootcamp*, available https://www.microsoft.com/en-us/research/event/private-ai-bootcamp/, (Last visited on September 14, 2022).

feedback and scores from experts. There are also social events where all participants have a chance to meet and network with other PhD students and experts from MSR.

The Caltech Artificial Intelligence and Machine Learning Bootcamp[184] showcases Caltech CTME's academic excellence and IBM's industry prowess. It boosts career opportunities for technology professionals by imparting vital skills and data literacy in Statistics, Data Science with Python, Machine Learning, Deep Learning, Natural Language Processing, and Reinforcement Learning. 'Inzva', a BEV Foundation project, is a non-profit hacker community organising study and project groups as well as camps in the fields of AI and Algorithm, and gathering CS students, academics and professionals in Turkey. It partnered with Google Developers in July 2022 to organise Google Developers Machine Learning Bootcamp.[185] This global project was organised in Turkey along with many other places from around the world including India, Japan, Latin America, South Korea and Europe. Apart from the completion certificate, graduates were also offered job and internship opportunities at the end of the program.

In India, Bahadur Chand Munjal Charitable Trust, realising that this century needs critical thinking, creativity, and innovation, has embarked on a mission to provide AI education with hands-on experience to students of grades III - IX. Here, the aim is to first teach the basics of programming, artificial intelligence, and machine learning. After this basic training, students compete in the competition where they make a project to win educational AI and robotics kits. [186] With the objective of building AI readiness among the youth of our country, the National e-Governance Division, Ministry of Electronics and Information Technology, Government of India, in collaboration with Intel India, has launched 'Responsible AI for Youth 2022'- A National Program for School Students[187]. The program aims to enable school students with AI skills, further democratising access to relevant toolsets to develop meaningful social impact solutions in various themes and eventually becoming responsible users of AI. The program is designed to provide learners with an opportunity to become part of the skilled workforce in an AI-fueled economy.

[184] Caltech Center for Technology and Management Education, *Caltech Artificial Intelligence and Machine Learning Bootcamp*, available https://ctme.caltech.edu/programs-for-individuals/data-analytics-open/ai-machine-learning-bootcamp-certificate-open, (Last visited on September 14, 2022).

[185] Inzva, *Google Developers Machine Learning Bootcamp*, available https://inzva.com/2022/ai/bootcamps/google-developers-machine-learning-bootcamp, (Last visited on September 14, 2022).

[186] Mission AI, *AI Bootcamps - Learn & Win*, available https://ai.bcmf.in/, (Last visited on September 14, 2022).

[187] Responsible AI for Youth 2022, available https://responsibleaiforyouth.negd.in/about, (Last visited on September 14, 2022).

Need for bootcamps in India

Bootcamps give an opportunity to work with a global team of innovators to build and deliver value through innovation. Active participation in international bootcamp programs such as MIT Bootcamps, Design Thinking Bootcamp by Stanford University etc. will help India's telecom industry find an international community of AI developers, navigate challenges and learn from experiences of others. It has been observed that organisations and companies have been organising Bootcamps to impart better skills to the workforce and to improve the overall performance of the organisations.

On a similar line, the industries in India may explore launching boot camp programs for AI and ML to build students and employees for development of solutions or products on AI in the telecom sector. While both governmental and private organisations may launch such programs, considerations of data protection will have to be kept in mind in case of private players. Imparting knowledge to students from a young age will also help them get acquainted with various international data regulatory frameworks.

Proposals and Suggestions

1. Training, Conferences, and Awareness Programmes:

The periodic training and knowledge-sharing conferences have to be conducted to ensure uniformity and be constantly responsive to the changing nature of the challenges posed by emerging technologies and other technological advancements. These awareness programmes may be in the form of bootcamps. Such training and conferences may be organised by Academic Institutions in collaboration with NETRA and technology developers and deployers. Separate and joint training programmes and conferences may be organised for Compliance Officers, Adjudicating Officers, recognised members of the Compliance Assistance Cell, Sectoral regulators, academia, etc. Awareness programmes for the general public may also be arranged as part of public outreach initiatives of NGOs and academic institutions.

The law, technology and management universities and institutions may contribute in developing certain modules for raising awareness among different stakeholders concerning legal requirements and mandated compliances and adoption of technological and management measures.

2. Generation of Funds through CSR:

To incentivise the developers and deployers undertaking any projects and are meaningfully and resourcefully contributing to further the initiatives of the NETRA, their contribution may be treated as their compliance of their statutorily mandated activities as part of corporate social responsibility (CSR).

3. E-Tech Data Library:

Organising bootcamps will also aid in contributing to the availability of literature in the area of research and development in AI. Compiling and storing of data can be done by the E-Tech Wing of the NETRA. Various initiatives under this wing, such as the E-Tech Data Library and E-Tech Lighthouse can help boost innovation and create an eco-system for encouraging participation in development and deployment of emerging technologies. Furthermore, the Compliance and Oversight Wing will also have a role to play in ensuring that control over the personal data of individuals is not compromised and that bootcamps organised by private bodies do not result in violations of some rights of the individuals.

Annexure A: Some details about sectorial regulators in India

Sr. No.	**Parent Act**	**Regulatory body name**	**Body composition**	**Role and responsibilities**
1.	It is a not-for-profit body set up by The Societies Registration Act, 1860.	Internet and Mobile Association of India ("IAMAI")	Composition of the board: - Chairperson - 3 Expert Members - 3 Signatory Members.	Under Rule 9(gg), the draft code provides that the Board shall pass a decision within 30 days of registration of a grievance. Such a decision shall either "*dismiss the Registered Grievance with prejudice*" or *"find that the concerned signatory must either reinstate or block access to the user account(s)..."*. The decision passed by the Board, shall include the specific URL identifying the information or content, reference of the Signatory's terms of service which was applied to arrive at the decision and the reasons for passing the decision.
2.	THE PERSONAL DATA PROTECTION BILL, 2019	DATA PROTECTION AUTHORITY OF INDIA	Composition of the Authority - Chairperson - not more than six whole-time Members	The Chairperson of the Authority shall have powers of general superintendence and direction of the affairs of the Authority and shall also exercise all powers and do all such acts and things which may be exercised or done by the Authority under this Act.The Chairperson and Members of the Authority shall meet at such times and places and shall observe such rules and procedures in regard to transaction of business at its meetings including quorum at such meetings, as may be prescribed. (2) If, for any reason, the Chairperson is unable to attend any meeting of the Authority, any other member chosen by the Members present at the meeting, shall preside the meeting. (3) All questions which come up before any meeting of the Authority shall be decided by a majority of votes of the Members present and voting, and in the event of an equality of votes, the Chairperson or in his absence, the member presiding, shall have the right to exercise a second or casting vote. (4) Any Member who has any direct or indirect pecuniary interest in any matter coming up for consideration at a meeting of the Authority shall disclose the nature of his interest at such meeting, which shall be recorded in the proceedings of the Authority and such member shall not take part in any deliberation or decision of the Authority with respect to that matter.

3	Securities and Exchange Board of India Act, 1992	Securities and Exchange Board of India	Composition of SEBI board - nine members. - One Chairman of the board (Central gov) - One Board member (RBI) - Two Board members (Ministry of Finance) - Five Board members (Central Gov)	It functions to fulfill the requirements of three categories – Issuers – By providing a marketplace in which the issuers can increase their finance. Investors – By ensuring safety and supply of precise and accurate information. Intermediaries – By enabling a competitive professional market for intermediaries. By Securities Laws (Amendment) Act, 2014, SEBI is now able to regulate any money pooling scheme worth Rs. 100 cr. or more and attach assets in cases of non-compliance. SEBI Chairman has the authority to order "search and seizure operations". SEBI board can also seek information, such as telephone call data records, from any persons or entities in respect to any securities transaction being investigated by it. SEBI performs the function of registration and regulation of the working of venture capital funds and collective investment schemes including mutual funds. It also works for promoting and regulating self-regulatory organizations and prohibiting fraudulent and unfair trade practices relating to securities markets.
4.	Aadhar Act, 2016	UIDAI	Composition of the Authority - two part-time Members and - one Chief Executive Officer	

5.	The Telecom Regulatory Authority of India Act 1997	Telecom Regulatory Authority of India	Composition of the Authority - one Chairperson, - not more than two whole time members - not more than two-part time members (central gov.)	To make recommendations, either suo motu or on a request from the licensor, on the following matters, namely:- i. need and timing for introduction of new service provider; ii. terms and conditions of license to a service provider; iii. revocation of license for non-compliance of terms and conditions of license: iv. measures to facilitate competition and promote efficiency in the operation of telecommunication services so as to facilitate growth in such services. v. technological improvements in the services provided by the service providers. vi. type of equipment to be used by the service providers after inspection of equipment used in the network. vii. measures for the development of telecommunication technology and any other matter relatable to telecommunication industry in general; viii. efficient management of available spectrum; (b) discharge the following functions, namely:- i. ensure compliance of terms and conditions of license; ii. notwithstanding anything contained in the terms and conditions of the license granted before the commencement of the Telecom Regulatory Authority of India (Amendment) Act,2000, fix the terms and conditions of inter-connectivity between the service providers; iii. ensure technical compatibility and effective inter-connection between different service providers. iv. regulate arrangement amongst service providers of sharing their revenue derived from providing telecommunication services; v. lay down the standards of quality of service to be provided by the service providers and ensure the quality of service and conduct the periodical survey of such service provided by the service providers so as to protect interest of the consumers of telecommunication services; vi. lay down and ensure the time period for providing local and long distance circuits of telecommunication between different service providers; vii. maintain register of interconnect agreements and of all such other matters as may be provided in the regulations;

6.	Payment and Settlement Systems Act, 2007 (PSS Act)	Board for Regulation and Supervision of Payment and Settlement Systems (BPSS), a sub-committee of the Central Board of RBI is the highest policy making body on payment systems in RBI.	Composition - Governor of the Bank who shall be the Chairperson of the Board - Deputy Governors of the Bank, out of whom the Deputy Governor who is in charge of the Department of Payment and Settlement Systems, shall be the Vice-Chairperson of the Board - Not more than three Directors of the Central Board - Two Executive Directors - permanent or ad hoc invitees.	Functions and powers of the Board.-(1) The functions and powers of the Board shall pertain to the regulation and supervision of payment systems under the Act. (2) In particular and without prejudice to the generality of the foregoing provisions, the functions and powers of the Board shall include the following matters, namely: (a) the laying down of the policies relating to the regulation and supervision of the payment systems including electronic, non-electronic, domestic and cross-border payment systems affecting domestic transactions; (b) the laying down of the standards for both existing and future payment systems; (e) the authorization of the payment systems; (d) the determination of the criteria for membership of the payment systems including continuation, termination and rejection of membership: (e) overseeing the administration of regulations and guidelines framed under the Act for the purposes of the above matters and the directions issued by the Bank from time to time to the operators of the payment systems and their members and taking such action as may be deemed necessary for ensuring the compliance; creating necessary administrative structure within the existing rules and regulations for ensuring effective regulation and supervision of the payment systems; (g) such other matters as are deemed necessary for the effective regulation and supervision of payment systems.

7.	The Pension Fund Regulatory & Development Authority Act 2013	The Pension Fund Regulatory & Development Authority	Composition of the Authority - Chairperson - three whole-time members - three part-time members (central gov)	The Chairperson shall have the powers of general superintendence and direction in respect of all administrative matters of the Authority. 9. (1) The Authority shall meet at such times and places and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be provided by regulations. the Authority shall have the duty, to regulate, promote and ensure orderly growth of the National Pension System and pension schemes to which this Act applies and to protect the interests of subscribers of such System and schemes. https://financialservices.gov.in/sites/default/files/PFRDA%20Act%202013_0.pdf

8.	IRDAI Act, 1999	IRDAI	Composition of the Authority - Chairperson; - not more than five whole-time members - not more than four part-time members (central gov.)	
9.	National Bank for Agriculture and Rural Development (NABARD) Act 1982	NABARD	Composition of The Board of Directors of the National Bank - Chairman - three directors (central gov) - three directors from out of the directors of the Reserve Bank three directors from amongst the officials of the Central Government	The general superintendence, direction and management of the affairs and business of the National Bank shall vest in a Board of Directors, which shall exercise all powers Managing Director shall have powers of general superintendence, direction and management of the affairs and business of the National Bank and may also exercise all powers. whole-time director appointed under sub-section (3) of section 6 shall assist the Managing Director in the discharge of his functions under sub-section (3) and perform such duties as the Board may entrust or delegate to him.

10.	the Food Safety and Standards Act, 2006	**FSSAI**	The composition of the Food Authority - Chairperson - twenty-two members out of which one-third shall be women. namely:- - seven Members, not below the rank of a Joint Secretary to the Government of India - two representatives from food industry - two representatives from consumer organisations - three eminent food technologists or scientists - five members to be appointed by rotation every three years - two persons to represent	The Central Advisory Committee shall ensure close cooperation between the Food Authority and the enforcement agencies and organisations operating in the field of food. The Chief Executive Officer shall be the legal representative of the Food Authority and shall be responsible for – (a) the day-to-day administration of the Food Authority; (b) drawing up of proposal for the Food Authority's work programmes in consultation with the Central Advisory Committee; (c) implementing the work programmes and the decisions adopted by the Food Authority; (d)ensuring the provision of appropriate scientific, technical and administrative support for the Scientific Committee and the Scientific Panel; (e) ensuring that the Food Authority carries out its tasks in accordance with the requirements of its users, in particular with regard to the adequacy of the services provided and the time taken; 13 (f) the preparation of the statement of revenue and expenditure and the execution of the budget of the Food Authority; and (g) developing and maintaining contact with the Central Government, and for ensuring a regular dialogue with its relevant committees.) It shall be the duty of the Food Authority to regulate and monitor the manufacture, processing, distribution, sale and import of food so as to ensure safe and wholesome food.

			farmers' organisations one person to represent retailers' organisations.	
11.	The Competition Act, 2002	Competition Commission of India	Composition of The Commission - Chairperson not less than two and not more than six other Members (Central Government)	https://www.cci.gov.in/legal-framwork/act (ref. pg 18-33)
12.	The National Highways Authority of India Act, 1988	NHAI	Composition of the Authority shall consist - Chairman - not more than six full-time members not more than six part-time members.	https://legislative.gov.in/sites/default/files/A1988-68.pdf (Ref. ch 3,4 and 6)
13.	Water (Prevention and Control of Pollution) Act, 1974.	CPCB	Composition of the Central Board - a full-time chairman (Central Government) - 1 [such number	Subject to the provisions of this Act, the main function of the Central Board shall be to promote cleanliness of streams and wells in different areas of the States. (2) In particular and without prejudice to the generality of the foregoing function, the Central Board may perform all or any of the following functions, namely:— (a) advise the Central Government on any matter concerning the prevention and control of water pollution; (b) co-ordinate the activities of the State Boards and resolve disputes among them; (c) provide

			of officials, not exceeding five,] to be nominated by the Central Government - such number of persons, not exceeding five, to be nominated by the Central Government - 2 [such number of non-officials, not exceeding three,] to be nominated by the Central Government - two persons to represent the companies or corporations owned, controlled or managed by the Central Government - a full-time member-secretary to be appointed by the Central	technical assistance and guidance to the State Boards, carry out and sponsor investigations and research relating to problems of water pollution and prevention, control or abatement of water pollution; (d) plan and organise the training of persons engaged or to be engaged in programmes for the prevention, control or abatement of water pollution on such terms and conditions as the Central Board may specify; (e) organise through mass media a comprehensive programme regarding the prevention and control of water pollution; 1 [(ee) perform such of the functions of any State Board as may be specified in an order made under sub- section (2) of section 18;] (f) collect, compile and publish technical and statistical data relating to water pollution and the measures devised for its effective prevention and control and prepare manuals, codes or guides relating to treatment and disposal of sewage and trade effluents and disseminate information connected therewith; (g) lay down, modify or annul, in consultation with the State Government concerned, the standards for a stream or well: Provided that different standards may be laid down for the same stream or well or for different streams or wells, having regard to the quality of water, flow characteristics of the stream or well and the nature of the use of the water in such stream or well or streams or wells; (h) plan and cause to be executed a nation-wide programme for the prevention, control or abatement of water pollution; (i) perform such other functions as may be prescribed. (3) The Board may establish or recognise a laboratory or laboratories to enable the Board to perform its functions under this section efficiently including the analysis of samples of water from any stream or well or of samples of any sewage or trade effluents.

			Government..	
14.	IBC,2016	IBBI	Composition of the Board - Chairperson; - three members from amongst the officers of the Central Government not below the rank of Joint Secretary or equivalent - one member to be nominated by the Reserve Bank of India, ex officio five other members to be nominated by the Central Government, of whom at least three shall be the whole-time members.	Refer Chapter 2 of IBC Act

15.	Cinematograph Act 1952	CBFC	- Chairman not less than twelve and not more than twenty-five other members appointed by the Central Government.	The Central Government may, by generral or special order, direct that any power, authority or jurisdiction exercisable by the Board under this Act shall 3 [in relation to the certification of the films under this Part] and subject to such conditions, if any, as may be specified in the order, be exercisable also by the Chairman or any other member of the Board, and anything done or action taken by the Chairman or other member specified in the order shall be deemed to be a thing done or action taken by the Board. For the purpose of exercising any of the powers conferred on it by this Act, the Central Government 5 [the Tribunal] or the Board may require any film to be exhibited before it or before 6[any person or authority] specified by it in this behalf.
16.	Small Industries Development Bank ,1990	SIDBI	- chairman and managing director appointed by the Central Government - two whole-time directors appointed by the Central Government - two directors who shall be officials of the Central Government nominated by the Central Government - three directors to	

			be nominated - three directors such number of directors not exceeding four elected in the prescribed manner	
17.	The National Housing Bank Act, 1987	National Housing Bank	- Chairman and a Managing Director - two directors - two directors, - two directors elected - one director - three directors from amongst the officials of the Central Government - two directors from amongst the officials of the State Government	Ref Ch. VII (PG 59-62) , Ch V (pg 30-31), Ch IV

Annexure B: List of other Accrediting Authorities in India

Sr. No.	Domestic Authority	Remarks
1.	National Payments Corporation of India_(NPCI)[1]	Architecture framework with a set of standard Application Programming Interface (API) specifications to facilitate online payments. NPCI authorizes and accredits various UPI applications.
2.	Standardization Testing and Quality Certification Directorate, Government of India, Ministry of Electronics & Information Technology[2]	● Safety Certification ('S' Mark) scheme is a third-party Certification scheme in the electronics sector promoted by STQC Certification Service[3] ● This scheme is intended to provide an adequate level of confidence, by means of system assessment, product testing, and subsequent surveillance, that the product conforms to the specified requirements of appropriate Safety standard published by International Electro-technical Commission (IEC). ● It also issues the CQW (certified quality website) mark which is a recognition that the website complies with the requirements of GIGW and the organization has adequate procedures and processes in place to provide reliable and dependable information and service through its website.[4]
3.	CBFC, Ministry of Information and Broadcasting[5]	The body outlines a stringent certification procedure for commercial movies screened in public places. Only films that have been edited and certified by the board can be broadcasted in public theaters and on television.[6]

[1] https://www.npci.org.in/who-we-are/csr/about-csr

[2] Stqc.gov.in

[3] https://www.stqc.gov.in/safety-certification-scheme-s-mark

[4] https://www.stqc.gov.in/website-quality-certification-0

[5] https://www.cbfcindia.gov.in/main/

[6] https://www.cbfcindia.gov.in/main/certification.html

Sr. No.	Domestic Authority	Remarks
4.	FSSAI [7]	FSSAI Registration, which is essentially a food safety certificate distributed by the food authority in India, assures the security of food products.[8]
5.	Directorate of Marketing and Inspection, Government of India[9]	AGMARK is a certification, issued by DMI, Govt. of India, employed on agricultural products in India, assuring that they conform to a set of standards. [10]
6.	Ministry of Commerce and Industry [11]	Issues GI tags - a sign used on products that have a specific geographical origin and possess qualities or a reputation that are due to that origin.[12]
7.	Ministry of Food Processing Industries, Government of India [13]	MIFPI issues the FPO certification on all processed fruit products sold in India such as packaged fruit beverages, fruit-jams, squashes, pickles, dehydrated fruit products, and fruit extracts. An FPO license is necessary to start a fruit processing industry in India.[14]
8.	Bureau of Indian Standards (BIS)[15]	Certifications[16]: ● A standard-compliance mark for industrial products is the ISI-ISI mark. Certain goods, including numerous electrical ones like switches, electric motors, wiring cables, heaters, kitchen appliances, etc., as well as others like Portland cement, LPG valves, LPG cylinders, automotive tyres, etc., must bear the ISI mark in

[7] https://www.fssai.gov.in/
[8] https://cleartax.in/s/fssai-registration
[9] https://dmi.gov.in/
[10] https://dmi.gov.in/
[11] https://commerce.gov.in/
[12] https://www.ipindia.gov.in/gi.htm
[13] https://www.mofpi.gov.in/
[14] https://www.mofpi.gov.in/sites/default/files/fpo_policy_process_guidelines_1_april_2013.pdf
[15] https://www.bis.gov.in/
[16] https://www.bis.gov.in/index.php/product-certification/products-under-compulsory-certification/

Sr. No.	Domestic Authority	Remarks
		order to be marketed in India. ● BIS Hallmark certifies the gold's purity. ● Ecomark - to goods confirming a set of guidelines intended to have the least possible impact on the environment.
9.	Central Pollution Control Board[17]	CPCB issues the Non-Polluting Vehicle mark. The mark attests to the motor vehicle's compliance with the applicable Bharat Stage emission requirements.

[17] https://cpcb.nic.in/

Annexure C: **Programs related to AI/ML currently being offered by various institutions and universities in India**

IITs:

- Powai (Bombay)
- Madras
- Delhi
- Kanpur
- Kharagpur
- Roorkee
- Guwahati

NIT

- Surathkal

IIIT

- Hyderabad

IISc Bangalore: M. Tech in artificial intelligence

- The master's program aims to enable students to develop an in-depth understanding of the technology and gather strong background and experience in it.
- The program offers a diverse group of electives and core courses including Data structures and Algorithms, Computer Vision, Reinforcement Learning, Deep Learning, Cryptography, and many more.
- COE: It is offered by the Artificial Intelligence Research center at the IISC

IITs

PLACE	COURSE OFFERED	COE/Dept.
Kanpur	● IIT Kanpur announced in May this year that its board has approved a four-year Bachelor of Science program, and a five-year integrated Masters of Science program in Statistics and Data Science ● The programs will focus on Computational and Data Science application courses and fundamentals of Statistics and Mathematics. ● It will allow students to select elective courses from the Department of Computer Science and Engineering and Electrical Engineering and is aimed at helping students master Big Data analytics.	Dept of mathematics and statistics

Bombay	● Certificate program in Machine learning & AI with python course gives a clear insight into python, Machine learning, neural networks, and natural language processing. ● Applicants study, analyze, and rearrange data and build Dataframes from scratch. ● Applicants will be taught to construct predictive linear models. ● Machine learning algorithms are taught with an understanding of mathematical and statistical models ● Understanding reinforcement learning. ● Linear classifiers and deep learning are taught to build text classification system	
Roorkee	● IIT Roorkee launched two new MTech programmes ● The programmes, MTech in AI and MTech in Data Science, aim to advance the AI and data science applications and studies in the country, promoting training and development of human resources, applied research, entrepreneurship and innovation.	CAIDS: Centre for artificial intelligence and data science
Madras	● Fellowship in AI for social good ● MTech in AI and MTech in Data Science, aim to advance the AI and data science applications and studies in the country, promoting training and development of human resources, applied research, entrepreneurship and innovation. ● a 12-weeks AI course on the National Programme on Technology Enhanced Learning (NPTEL) platform, called 'Artificial Intelligence Search Methods for Problem Solving.' Professor Deepak Khemanu will deliver the sessions from the Department of Computer Science and Engineering at IIT Madras.	Robert Bosch Centre for Data Science and AI and Narayanan Family Foundation
Delhi	● PGD in data sciences and AI ● The course will equip students with the fundamentals of statistical analysis, mathematical analysis and	

	optimisation; fundamental and advanced machine learning and deep learning; data engineering techniques; handling big data; in-depth understanding of various business application domains.	
Kharagpur	● The Centre for Artificial Intelligence started in April 2018. It has a four fold mission. ● Excellence in Artificial Intelligence Research ● Applied Artificial Intelligence: To build a vibrant community of professors, researchers and students that apply AI to solve real industry specific problems. ● Teaching and Outreach in Artifcial Intelligence and Machine Learning ● Research based Entrepreneurship	The Centre for Artificial Intelligence ai.iitkgp.ac.in
Guwahati	Various courses offered: Btech, internships, online training courses. Details regarding manifold courses can be found here: https://eict.iitg.ac.in/online_courses_training.html	

NITs

Suratkhal	NIT Karnataka, Surathkal, recently announced that the Academic Senate, Board of the institute, and Union Ministry of Education has approved a new four-year BTech course in AI.	Department of Information Technology

IIITs

Place	Course offered	COE

Hyderabad and Talent Sprint (TalentSprint is a National Stock Exchange group company that is based in Hyderabad. It partners with academic institutions and corporations to offer certificate programs to improve the technology industry.)	● It is a packaged course that offers dual certification and career guidance. One can expect to become a full-fledged Artificial Intelligence and Machine learning developer. ● They offer hands-on projects that further engrain the technical know-how. ● Applicants are introduced to 7 tools: Hadoop, PyTorch, Spark, CI/CD, etc. ● Career development includes one on one career monitoring, mock interviews, and guidance on the project presentation	

BITS Pilani: This is an 11 months long online PG program that can also be pursued by working professionals. The program can be accessed to improve the knowledge base and skills in AI and machine learning. The syllabus covers key concepts of these technologies and consists of 6 courses.

About Universities Abroad:

University	**Courses**	**COE**
Cornell University	AI policy and ethics	Center for Data Science for Enterprise and Society
Harvard University	● The Ethics and Governance of Artificial Intelligence(No exam, reading group) ● CS50's Introduction to Artificial Intelligence with Python (CS) ● Competing in the Age of AI—Virtual (Business) ● Designing and Implementing AI Solutions for Health Care (DS)	Berkman Klein Center

MIT	● Artificial Intelligence (Primer) ● Artificial Intelligence: Implications for Business Strategy (Business) ● Professional Certificate Program in Machine Learning & Artificial Intelligence	● MIT Computer Science and Artificial Intelligence Laboratory ● MIT Institute for Data, Systems, and Society ● Laboratory for Information and Decision Systems
Columbia	Artificial Intelligence Certificate Program (Primer)	
Penn	Artificial Intelligence	● AI for Cyber Security through Big Data ● Algorithmic Learning, Privacy and Security (ALPS) Laboratory ● Artificial Intelligence Research Laboratory ● Center for Artificial Intelligence Foundations and Scientific Applications (CENSAI) ● Center for Big Data and Discovery Informatics ● Center for Socially Responsible Artificial Intelligence ● Crowd-AI Laboratory ● Data Science and Machine Learning Lab ● FAIR Lab ● The RAISE Lab
Yale		Intelligent Computing Lab
Stanford	● AI for Social Good ● Artificial Intelligence: Principles and Techniques ● Design for Artificial Intelligence ● Artificial Intelligence in Healthcare ● Ethics of AI ● Value of Data and AI ● Graphics in the Era of AI ● Artificial Intelligence for Disease Diagnosis and Information Recommendations	Stanford Artificial Intelligence Laboratory

	- Seminar on Artificial Intelligence Safety - Seminar in Artificial Intelligence in Healthcare	
Oxford	Oxford Artificial Intelligence Programme (Primer)	https://www.research.ox.ac.uk/area/ai
Cambridge	Cambridge AI offers a variety of courses	- Cambridge AI Centre - Cambridge University Artificial Intelligence.
UC Berkeley	- CS188 Intro to AI (Primer)	Berkeley Artificial Intelligence Research