

NASSCOM & DSCI**feedback to the****Telecom Regulatory Authority of India (TRAI)****Consultation Paper on Leveraging Artificial Intelligence and Big Data in the
Telecommunication Sector****November 4, 2022**

The National Association of Software and Service Companies (**NASSCOM**) and the Data Security Council of India (**DSCI**) welcome the opportunity to submit our response to the Consultation Paper on “*Leveraging Artificial Intelligence and Big Data in the Telecommunication Sector*” (**Paper**) released by the Telecom Regulatory Authority of India (**TRAI**) in August 2022.ⁱ

General comments

First, the Paper covers considerable ground and has a wide scope, since it deals with the interplay of three concepts – Artificial Intelligence (**AI**), Big Data (**BD**), and the future of telecom networks – and their interplay all together.ⁱⁱ While the primary focus for the Paper was on AI & BD in telecomⁱⁱⁱ, it engages with many sector-agnostic aspects as well.^{iv} We appreciate the effort to adopt a comprehensive approach. However, we do find that, at various places, it is not clear what is the context of a particular question from a telecom policy or regulatory perspective. For example, the first question asks on what the most appropriate definition of AI can be. It is unclear whether this was posed more to understand the state of the art or to frame a definition for a future telecom policy or regulatory initiative.

Second, several questions focus on examining how telecom and next-generation networks could enable the adoption of AI & BD across sectors. We submit that there are two separate issues: (1) the sector-specific adoption of AI & BD within telecom and next-generation networks (2) the sector-agnostic adoption of AI & BD across sectors, where telecom and next-generation networks are one of the many enablers. In both cases, firms and governments will require several enablers, capabilities, and resources, including network connectivity, data, and talent, to leverage AI & BD to their fullest. This is to be kept in mind when framing future policies or regulations: that we do not over-emphasise one enabler (here, networks) over others. This also points towards a need for a more cohesive and integrated approach to AI & BD policy and regulation going forward. We need multiple stakeholders to collaborate, so that such initiatives are not limited in scope by sector-specific or enabler-specific perspectives. We discuss this further in our responses to chapter 4 below.

Specific comments to the issues for consultation

In this section, we provide our responses to the issues for consultation. Since the Paper covers much ground, our approach has been to provide consolidated responses on the questions raised in each section of the Paper. The sections are arranged chapter-wise, except for chapter 5, the largest chapter, which we have sub-divided our responses as per its sub-sections. We have also **underlined** which parts of each of the questions our responses are focusing on.

Chapter 2: Introduction to Artificial Intelligence and Big Data

- Q1. What may be the most appropriate definition of Artificial Intelligence (AI)? What are the broad requirements to develop and deploy AI models in a telecom sector? Whether any major challenges are faced by the telecom service providers in adopting AI? Please justify your response with rationale and global practices, if any.
- Q2. Whether the big data in the telecom sector may be utilised for developing AI models? For efficient and effective handling of big data, whether there is a need for adoption of special programming models or software frameworks? Please justify your response with suitable examples and global practices, if any.
- Q3. Whether deployment of 5G and beyond technologies will help to accelerate adoption of AI in all the sectors and vice versa? Please justify your response with suitable illustrations including global practices, if any.
- Q4. 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.
-

Response:

The definition of artificial intelligence

As the Paper notes as well, a universally accepted or applicable definition of AI does not exist. A major reason for this is that the term ‘AI’ does not refer to one single thing. It may be used to refer to the *academic discipline* or field of inter-disciplinary study, that draws from the cognitive, statistical, and computer sciences. AI can also be used to refer to *models*, namely, specific software programs that implement algorithms studied in different fields, such as computer vision or machine learning.^v AI can also be used to refer to *automated decision-making systems*, which are technical systems used to aid or augment human decision-making, often using AI models.^{vi} It may also be used in more general terms to refer to a *wide variety of applications* that are seen to enable machines to perform a task that is associated with human intelligence, such as reasoning or pattern recognition.^{vii}

We point this out to demonstrate the challenge with trying to arrive at an ‘appropriate’ definition of AI – that the ‘appropriateness’ of the definition depends on what precisely is being referred to and why the definition is required. The question in the paper does not provide any context to the use of the definition. If it is intended to be used to define regulation or a law, then we would suggest that, rather than trying to define AI, it is better to define the application or product that is sought to be addressed. This is because, in practice, AI systems are built, not as “general-purpose” systems, but as domain-specific systems designed for specific tasks, and are, therefore, not comparable.

So, for example, the analysis of self-driving cars is extremely different to that of surgical robots.^{viii} Thus, rather than trying to define whether a self-driving car is an AI system or not, it is important

for regulations to incentivise safe driving outcomes and penalise harms on account of unsafe driving behaviour and contextualise these motivations to different types of AI systems with varying capabilities.^{ix} A general definition of AI for a legal instrument may also risk only serving a symbolic purpose – a criticism of the European Commission’s draft Artificial Intelligence Act, where the general definition of AI offers little in terms of clarity, and where the actual material scope of the draft law is defined by a list of specific applications contained in its Annexures.^x

Perhaps the lack of a precise, universally accepted definition of AI probably has helped the field to grow and advance.^{xi} To elaborate, subtle differences in definition can have major impacts on some of the most important problems facing policymakers.^{xii} For instance, automation and AI sound similar, but may have vastly different impacts on the future of work.^{xiii} Similarly, there is a risk that traditional software which are quite different from AI, may end up getting covered within the scope of a broad definition of AI.^{xiv} These can have unintended outcomes like, regulatory excess, overlap and/or ambiguity and unnecessary costs. Globally such risks are being recognised, and therefore, we must too.

The difficulty with adopting a single definition of AI has also been acknowledged by multiple countries. The UNESCO, in its Recommendations on the Ethics of Artificial Intelligence (**UNESCO Recommendations**), adopted in 2021, did not try to adopt a single definition of AI, noting that such a definition would need to change over time with technological change.^{xv} It instead focused on identifying three features of AI systems that, as per the recommendations, are of central ethical relevance. These are that: (1) AI systems are designed to operate with varying degrees of autonomy and across domains (2) ethical questions arise across all stages of the AI system life cycle and (3) AI systems can raise a wide range of ethical issues.^{xvi}

The development of multiple terminologies for a principled approach to AI

We agree that there are overlaps between the various terminologies that have been coined by various organisations and nations to address challenges related to trust with AI. By one estimation from 2019, there were at least 84 documents containing principles or guidelines for AI, and 88% of these were released after 2016.^{xvii} The Paper notes a few, such as “Responsible AI”, “Explainable AI” or “Trustworthy AI”, which are all frameworks intended to normatively guide the design, development, and deployment of AI systems using a principled approach, so that they are ethical and add value to individuals and society [see section 2.5]. The Paper also lists a number of terms, such as generative AI, augmented AI, or embedded AI, in the same list, but we find these to be different from the first three examples, since they refer more to potential capabilities that can be enabled through AI. It is important, we submit, not to confuse these two different concepts (principles and new capabilities).

Focusing on the principles, and on the question of whether there is a need to *define* or *harmonise* these terms, we submit that any such exercise should not be focused on trying to impose a common understanding across stakeholders. Such standardisation may not add much value as it would ultimately only add one more framing of a principled approach to AI. The field is also not mature enough to have reached the stage where a specific practice of a principled approach to AI can be mandated across the board. Instead, we suggest that the TRAI may take up the exercise of identifying common themes that underpin the various existing terminologies available today and make such a thematic mapping generally available to stakeholders.^{xviii} It would also be useful in building on such a mapping and contextualising these themes to the Indian context. This would be helpful for stakeholders to understand what the consensus of the underlying themes and the desired outcomes across themes in the Indian context is.

We are happy to assist in this regard. NASSCOM has already developed a set of [Responsible AI principles](#). While developing them, we noted that the major themes on which there is a degree of consensus are: (1) fairness (2) transparency (3) privacy & security (4) explainability (5) accountability (6) safety & reliability and (7) alignment with human values.^{xix} These may be considered as a starting point for conducting a more comprehensive thematic mapping.

Chapter 3: Opportunities and risks involved

- Q5. Which are the applications of AI and BD already being -used by the TSPs in their networks to improve Quality of Service, Traffic Management, Spectrum Management and for Security purposes? Please list out all such applications along with the level of maturity of such applications. Please specify whether they are at trial stage or pilot stage or have reached the deployment stage? Details should include type of AI models, methods to access data, and procedures to ensure quality of data.
- Q6. What are the major challenges faced by the telecom industry, including policy and regulatory, in developing, deploying, and scaling applications of AI listed in the response to Q.5? How can such challenges be overcome? Please justify your response with rationale and suitable examples, if any.
- Q7. In which areas of other sectors including broadcasting, existing and future capabilities of the telecom networks can be used to leverage AI and BD? Please justify your response with rationale and suitable examples if any.
- Q8. 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.
- Q9. 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.
- Q10. What measures do you suggest to instil trust and confidence regarding a robust and safe AI system among customers, TSPs and other related entities/stakeholders? Whether adopting general principles such as Responsible AI and ethical principles at the time of designing and operationalising the AI models will help in developing ethical solutions and instilling trust and confidence in the users? What may be such principles and who should formulate these and how compliance can be ensured? Please justify your response with rationale and suitable examples, if any.
- Q11. 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.
- Q12. 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.

Response:**Applications of AI & BD being used in telecom**

While we do not offer a comprehensive listing, we do suggest that, to analyse the different applications of AI & BD in the telecom sector, it is useful to distinguish between (1) sector-agnostic applications being used in the telecom industry and (2) sector-specific applications.

The Paper does do this to an extent when describing, in sections 3.2.1 to 3.2.4 and section 3.2.6, use-cases for AI in the telecom sector; these are clearly sector-specific applications. We agree, generally, with the various examples noted and have found that, in terms of sector-specific applications, we find that telecommunication service providers (**TSPs**) are using applications of AI & BD for two major purposes: (1) at the customer level, to understand the behaviour of customers and improve their user experience, such as by optimising network utilisation or developing customised pricing plans;^{xx} (2) at the network level, to improve network performance, such as by identifying gaps like high interference, poor coverage, low throughput, and design the right actions, like adding or changing cell towers, etc. AI & BD also help in anomaly detection and the prediction of service degradations.^{xxi}

We also note that there are several sector-agnostic applications being used by telecom players today to automate or improve various processes, such as business intelligence collection or compliance. These are not necessarily unique to the sector, since they can be leveraged by players in other sectors as well for similar benefits, but these are useful to consider as well. For example, a recent NASSCOM report highlights how an Indian contract analysis platform was able to use innovations in text analytics and computer vision to help a large telecommunications company review and manage the enforcement of a range of contracts, including tower leasing contracts, and increase productivity by 60% and save USD 20 million.^{xxii} In another recent report, NASSCOM has discussed a number of case studies where sector-agnostic AI platforms offered by Indian IT service companies are being used by telecom players.^{xxiii}

However, the Paper then also discusses, in section 3.2.5, use-cases for AI & BD for the broadcasting sector, and, in section 3.3 till section 3.4, how AI & BD, combined with future networks, can unlock opportunities for the telecom sector to offer more than connectivity to other sectors. The Paper discusses how the telecom industry can offer significant amounts of data, in terms of call data records and network records, to other sectors for AI development. In our view, the use cases need to be based on solutions designed to meet a real demand or interest from potential users. The regulatory discussion thereafter must be based on reasonably well identified risks and harms which merit a regulatory and enforcement intervention. In terms of data sharing, for personal data, there are non-trivial privacy risks posed by the sharing of such data at scale without a data protection law in place.^{xxiv} Similarly, there are risks associated with sharing of non-personal data. Data related risks are being examined by the government. AI related risks need to be determined and categorised in the telecom context, to engage in discussions on the way forward.

Addressing risks posed by AI systems

The Paper poses different questions on whether risks and concerns posed by applications of AI are acting as barriers to the adoption of AI & BD [see questions 6, 8]. We submit that, yes, risks and concerns do exist and like with any new technology, these do act as barriers to the adoption of AI & BD. We also agree with the approach of distinguishing between sector-agnostic risks [see

section 3.4.2] and sector-specific risks [see section 3.4.3]. However, beyond this, we wish to submit the following points on how such risks and barriers may be addressed.

The starting point must be to have a personal data protection law in place

As a starting point, two risks, that are well-understood but on which progress is limited, should be our priority to address: (1) *risks to informational privacy* and (2) *risks to data security*. It is essential to have in place a personal data protection law, since such a law can play a significant role in addressing privacy and data protection risks posed by AI systems. There are also several privacy-enhancing technologies (**PETs**) – enabling the encryption and masking of data – that can be deployed to both enhance and preserve privacy, using a privacy-by-design approach.^{xxv} A personal data protection law can provide the fillip necessary to ensure the adoption of these at scale.

Once such a law is in place, it would likely operationalise the setting up of a data protection regulator. This is a significant exercise to undertake, since, as we have seen in other countries, data protection regulators can play a significant role in working with other regulators or stakeholders to address risks posed by AI systems from different perspectives. A data protection regulator can, for example, consider how to contextualise data protection for developers of AI in India. It is worth noting that there are already self-regulatory initiatives undertaken in this regard, which such a regulator can look to learn from. For example, DSCI had, in July 2021, collaborated with other stakeholders to prepare a handbook with practical guidance for the responsible development of AI, especially from a privacy and data protection perspective. Such existing efforts can be leveraged by a future regulator to address privacy-related risks.^{xxvi}

Before new regulation, high-risk use-cases should be systematically identified

After addressing privacy and data security, the next step should be to conduct a granular risk-assessment exercise to identify the next level of risks posed by AI systems. In general, we recommend a risk-based approach, where high-risk use-cases are prioritised first.

Here, we note that much work has been done on analysing sector-agnostic concerns already, and while there are useful sector-agnostic frameworks to understand AI risk, at the end of the day, it is important to keep in mind that AI systems are often purpose-specific and are not comparable. This extends to the assessments of risks associated with the design and implementation of AI systems. For example, risks associated with AI models used for credit scoring would be different to those posed by AI systems used for network design in the telecom sector. There is limited value in only creating a list of risks that can be generalised across AI systems, since, beyond a point, this would be only an exercise in abstraction.

However, what can be standardised is the framework for risk assessment. There should be a single risk assessment framework to identify high-risk applications regardless of sector. Much work has also been done already on how to assess risk. We note that, in our response to a previous consultation paper released by the NITI Aayog, we had submitted that a suitable framework for understanding risk in the context of AI applications worth considering is the framework developed by the German Data Ethics Commission.^{xxvii} It is also important that both the sector and the intended use of an AI application needs to be considered for evaluating risks, in particular from the viewpoint of protection of safety, consumer rights, and fundamental rights.

Finally, after identifying and prioritising risks, it is important to ensure that, before new regulatory interventions are considered, that existing regulations are carefully analysed to identify gaps that need to be addressed. We already have several relevant laws in place, such as extant telecom and consumer protection regulation.^{xxviii} For example, with an effective personal data protection

law in place, it is possible that a number of consumer-centric harms posed by AI models will be addressed by regulations intending to address profiling or to require companies to adopt privacy-by-design. We generally recommend resisting over-regulation in anticipation.

Any new AI regulation should be risk-based and precise

As noted above, any new AI regulation should be developed after risks are clearly identified. Beyond this, we also recommend ensuring that regulation is *precise* and addresses actual gaps. We must be wary of the fact that a disproportionate intervention can impede the growth of the evolving AI ecosystem in India. Depending on the nature and intensity of risk and the enforcement gap, a targeted and precise mechanism/intervention may be designed thereafter.

It is also worth noting that we need not always jump to legislative efforts or new regulations from a regulator; self-regulatory or co-regulatory mechanisms can also work to address risks. There are several ongoing industries led initiatives to adopt measures to build trust and confidence regarding a safe AI among customers, TSPs and other stakeholders.

To illustrate, a recent [guide](#) developed by NASSCOM prescribes responsible AI best practices, implementation methods and can serve as a handbook for compliance with responsible AI principles at each stage of the lifecycle of an AI application.^{xxix} It is also important to keep in mind such initiatives when considering how principled approaches to AI may be enforced; self-regulatory efforts can be of much value, especially since the field is in its infancy in India.

The need for a new regulatory body

We submit that it is premature to look to set up a telecom/ICT sector specific or a common *regulator* to check and ensure compliance of national or sector-specific requirements for AI, or to enforce compliance with principled approaches to AI. In 2020, NASSCOM clarified its position on this aspect as part of the Feedback on the Discussion Paper^{xxx} issued by the Department of Telecommunications (DOT) on the Indian AI Stack^{xxxi} (**Indian AI Stack Feedback**). In this response, NASSCOM submitted that, since AI systems are used in multiple sectors, a sector regulator if any, may have the mandate to address issues that arise due to deployment of AI system in any sector.

We do note that there is a need for a *coordination mechanism* to ensure a *whole-of-government* approach can be achieved. As acknowledged in Annexure II of the Paper, there have been several consultation processes and initiatives across different Government bodies to examine AI (**Annexure II** lists out 14 different initiatives). As noted in recent reports, we have suggested that the Government of India look to establish or designate a dedicated and independent nodal body or office, with relevant subject matter expertise, and focusing on serving as a steering mechanism for national and inter-ministerial coordination on AI.^{xxxii}

The role of such a body or office can be to ensure that these various initiatives can come together and ensure a whole-of-government approach. Rather than regulation by default, it can look to prioritise instead ensure that we do not duplicate existing efforts further. Such a body can also run integrated consultation processes to solicit evidence on issues of relevance across government. It can also help different government initiatives come together to leverage the various initiatives and programs in the private sector in a unified manner. For example, as noted above, NASSCOM and DSCI have worked with a number of industry members and expert partners to build toolkits and best practices for enterprises to adopt a responsible AI approach^{xxxiii} or a privacy-preserving approach; these can be used by such a nodal body or office to build best practices across sectors. It may also function as the nodal agency for promoting

India's AI ecosystems, such as encouraging more indigenous R&D, or developing necessary local talent.^{xxxiv}

The UNESCO Recommendations contain key guidance on how AI governance mechanisms should be structured. They should be inclusive, transparent, multi-disciplinary, multi-lateral and multi-stakeholder. A dedicated nodal body or office should look to incorporate these features.^{xxxv}

The Paper asks on whether a new law is required to set up such a dedicated nodal body or office. We do not have a final position on this. To get there, we need better understanding of where the existing laws are falling short. For example, if we take the financial or health sector laws, we need to understand in detail the regulatory and enforcement gaps when it comes to dealing with the AI system related harms. Similarly, we must ask the industry, what kind of innovation or solutions are being restricted in the existing legal framework? This might help us focus on the right solution. We are happy to work with the TRAI and other relevant government stakeholders to identify the scope and mandate of such a body or office.

Chapter 4: Key constraints in adoption of AI & BD

- Q13. Whether telecom/ICT industry is facing constraints such as access to data, lack of computing infrastructure, lack of standards, and R&D in the adoption of AI and BD technologies? Please list out all such constraints with adequate details.
- Q14. What measures are required to make data and computing infrastructure available and accessible to developers and also to make data/AI models interoperable and compatible? Please respond along with examples, best practices and explanatory notes.
- Q15. Whether there is a gap between requirement and availability of skilled AI workforce? If so, what measures are required to be taken to ensure availability of adequate skilled workforce in AI domain? Please respond along with suggestions with supporting details and best practices.

Response:

Constraints facing the telecom & ICT industry in AI adoption

The Paper outlines both sector-agnostic and sector-specific constraints hindering the adoption of AI & BD in the country. We wish to emphasise the following. *First*, the need for greater emphasis on the implementation of open government data policies – to make data held by public sector bodies available to a larger ecosystem. In this regard, we request the TRAI to examine the recommendations offered to the Central Government by the Open Data Taskforce, an initiative anchored by NASSCOM.^{xxxvi} *Second*, as discussed already above, the need for both legal protections and technological solutions to address privacy and security risks. A starting point to addressing this gap is to introduce a data protection law and establish an independent data protection authority. This aligns with the observations in the Paper that the lack of formal regulation for data acts as a regulatory impediment [see section 4.3.4].

We do note that the Paper identifies three scenarios where regulatory intervention is required: (1) where industry is unable to realise or unleash the full potential of AI & BD in the instant case

(2) when direct or indirect harm is inflicted on others (3) when collaboration of stakeholders is required for creating a comprehensive ecosystem for implementation of solutions [see section 4.3.4]. Here, we are concerned about what is meant by “regulatory intervention” as against “government intervention”. It is important to remember that formal legislation or regulation be considered only when a market failure to be corrected is identified. It is also important to ensure we do not over-regulate; this requires ensuring interventions are targeted and address existing gaps in regulation, rather than duplicating existing requirements. For example, the start-up India initiative is a “government intervention” to help start-ups realise their potential; it is not a “regulatory intervention”.

On the issue of AI standards, we recommend that we should not end up in creating India specific standards, which are not interoperable with the rest of the world. AI, as a field, is at its early stage of growth and global public-private collaboration is crucial to avoiding overregulation. Currently, there are a few initiatives underway globally to develop international standards for different aspects of AI deployments. These include efforts that support responsible and ethical use of AI, such as the [Institute of Electrical and Electronic Engineers’ \(IEEE\) P7000 series and the ISO/IEC CD 23053.2](#) - both of which are still in the draft stage. Given this background and the nature of the technology, harmony and alignment with international standards is important to ensure that domestic companies do not face challenges to expand their business beyond India.

Availability of adequate skilled workforce in the AI domain

NASSCOM has been undertaking several initiatives to bridge employability and skilling gaps within the Indian IT industry; a specific focus has been placed on AI & BD under these initiatives. In a 2018 report, NASSCOM noted that there were already ~370,000 employed talent pool skilled in AI & BD in 2018; this was estimated to reach ~570,000 by 2021.^{xxxvii} As per a recent NASSCOM study, Bangalore already features in the top five cities with the largest AI talent pool.^{xxxviii} So, India is well-positioned in terms of availability of a skilled workforce for the AI domain.

However, there is still a lot of scope for capacity building in AI and need for alignment of skills of the AI workforce with the requirements of the industry. This would require several approaches. For example, it would require mapping curriculum at institutional levels with industry job roles/standards. We note that training in the domains of AI & BD should also incorporate social sciences, as these are vital to understand the societal impact that AI systems can have.

While the Paper raises several issues (in Chapter 5) on how to build an ecosystem in the AI space, at present the efforts in this regard are fragmented, and needs to be more aligned with the market. To address this, we need to design sector-specific AI solutions. For this, we need clear identification of existing AI problems, APIs, existing solutions/models in each vertical/sector. To ensure efforts/innovations are not duplicated, the entire set of curated information/data must be released in the public domain. Based on this readily available information, researchers, practitioners, and stakeholders can choose areas which needs further research and solutions.

Another strategy would be to build collaborations at the sectoral level between industry and students, so that directly adaptable skills for the industry can be built. Further, given the dynamic nature of the AI technology, syllabi would need to be periodically reviewed to remain relevant. Finally, more work is required to ensure inclusivity: that skills are distributed across all groups in society, with a particular focus on women and girls. As per the World Economic Forum, there is an increasing global trend of gender gap in AI skills.^{xxxix} Addressing these disparities explicitly in the skills framework will be essential.

Chapter 5: Enablers for adoption of AI & BD for cross-sector utilisation

Section 5.3. Data democratisation

- Q16. What initiatives do you suggest to democratise data required to develop AI models in the telecom sector? Please justify your response with rationale and suitable examples, if any.
- Q17. 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 need to be entrusted to generate and make available synthetic data? Please justify your response with rationale and suitable examples, if any.
- Q18. 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.

Section 5.4. Protecting privacy in an AI-driven world.

- Q19. (a) Which are the currently used privacy enhancing and privacy preserving technologies facilitating adoption of AI and BD? Are there any challenges in using these technologies? How these challenges can be addressed? (b) Which are the potential technologies likely to be available in near future to further strengthen privacy? Please justify your response with rationale and suitable examples, if any.
- Q20. Whether the list of technologies provided in response to Q.19 are adequate to handle all the perceived risks and concerns in the AI domain? Or is there a need to develop new privacy preserving architecture? Please justify your response with rationale and suitable examples, if any.

Response:

Data democratisation

As discussed above, we suggest that the primary strategy that should be taken up at this stage is to implement open government data policies and to identify high impact public good uses cases which can be enabled through availability and sharing of data. The use cases should drive the engagement to bring the industry, academia together to validate the use cases and build solutions. On the envisaged tasks for any regulatory body, we reiterate that, rather than a regulatory body, a coordination mechanism should be established [*please see our responses to chapters 3 and 4 above*].

We note here that the Paper envisages that a regulatory body may take up tasks that are similar to the proposed tasks envisaged for an Indian Data Management Office that has been proposed by the Ministry of Electronics and Information Technology.^{x1} This reiterates the need for coordination – we wish to avoid such initiatives overlapping.

Protecting privacy in an AI driven world

Please see our responses to chapters 3 and 4.

Section 5.5. Moving AI at edge

Whether the next generation telecom network architectures such as AI at edge, federated learning, TinyML or their combination can offer solutions to meet both privacy as well as intelligence requirements? Please justify your response with **rationale** and suitable examples, if any.

- Q21. What type of technological advancements are happening for running the AI models on the end user devices to overcome constraints in respect of processor, memory, battery etc.? Whether special tools, programming languages, and skills are required to be developed to build such AI models? Please justify your response with rationale and suitable examples, if any.
- Q22. Considering availability of new privacy preserving architectures as suggested in response to Q.19 and Q.20, what is the likelihood of emergence of new business and operational models? Whether such models will raise issues related to ownership and responsibilities? What do you suggest to address these issues? Please justify your response with rationale and suitable examples, if any.
- Q23. Whether the concept of “Operator Platform” would help in providing AI based solutions in a unified and more equitable manner? Apart from popular federated use cases of edge cloud federation, Cloud XR, Cloud Gaming, whether this concept may also be applied for public service delivery and in making public policies that are data-driven? Whether there is a need to take initiatives for developing and demonstrating advantages of concept of “Operator Platform”? If so, what steps and measures are suggested to launch such initiatives? Please justify your response with rationale and suitable examples, if any.

Section 5.6. Build AI specific infrastructure for telecom

- Q24. 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.
- Q25. Whether the emerging trends of development of foundational AI models such as GPT-3, Gopher etc. are leading to democratisation of AI space by offering fine-tuned or derived AI models? Whether such a trend will also help in reducing costs for the AI developers? Whether similar approach will help in development of large-scale AI model for the telecom sector? Please justify your response with rationale and suitable examples, if any.

Section 5.7. Mechanisms for Experimentation & Demonstration

- Q26. 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 enable them to focus on their core competence areas? Please justify your response with rationale and suitable examples, if any.
- Q27. 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.
- Q28. 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.

Response:

Designing experimental campuses

Yes, this is a welcome initiative. However, we have highlighted certain concerns in our response to Q no 15 which needs to be carefully considered while designing such experimental campus. We also recommend setting up virtual campus for a broader outreach and impact.

Introducing a regulatory sandbox

The Paper proposes introducing a regulatory sandbox to promote AI & BD innovations in the telecom sector. For such a sandbox to give promising results, clear guidance would be required on how it would operate. For this purpose, the government may draw guidance from the *Report of the Inter-ministerial Committee for Finalisation of Amendments of the Payment & Settlements Systems Act, 2007*^{xii} to provide the essential purpose, scope, and process of the sandbox.^{xiii} To illustrate, a regulatory sandbox must have detailed provisions on a range of matters, including, but not limited to the (1) process for applying to a sandbox (2) scope of a temporary exemption from a regulatory requirement applied for (3) factors to determine whether to grant the temporary exemption or not (e.g., innovation, benefit to consumers, risk, etc.) (4) conditions and time-period governing the exemption (5) need for the exempted entity to file a report after the sandbox period is completed (6) procedure for revocation of the exemption.

It would also be necessary to clarify what regulatory conditions could be waived – since, currently, the TRAI is not the only regulator in the telecom sector, and several obligations are enforced by the DOT. Both would need to be involved for the sandbox to work. This is necessary to provide certainty, clarity, and transparency to the prospective beneficiaries. We also note that regulatory sandboxes have been proposed under both the draft data protection law (which is for AI) and the new draft telecom bill (which is for the telecom sector), so the interplay between all these different initiatives would need to be clarified.

Section 5.8. Conducting challenge-based program

- Q29. Whether active participation in the international challenge programs such as ITU 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.
- Q30. 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.

Section 5.9. Adoption of MLOps (Machine Learning Operations) and Tooling

- Q31. Whether the telecom industry is required to adopt a Machine Learning Operations (MLOps) environment to develop, train, validate and store ML models? Whether there is also a need to establish a DataOps feature store to help MLOps for training purposes? What standardisation is required in terms of interoperability and compatibility for MLOps to function in a federated manner? Please justify your response with rationale and suitable examples, if any.

Section 5.10. Making AI workforce

- Q32. 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.
- Q33. 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.

Response:

Existing courses or programs related to AI & machine learning

We recommend examining how curricula on AI ethics can be developed across all levels, and how cross-collaboration between AI technical skills education and humanistic, ethical, and social aspects of AI education can be promoted. Online courses and digital resources on AI ethics education should be developed in local languages, including indigenous languages, and

consider the diversity of the environments, especially ensuring accessibility of formats for persons with disabilities. Further, the experience of global bodies like UNESCO and OECD^{xliii} indicate that the traditional way of imparting knowledge has evolved, especially in the digital domain. For instance, opportunities for more flexible, shorter-term, and targeted learning opportunities and modalities have proliferated in recent years. This is due to their uptake, opportunities anywhere they offer in terms of self-learning (e.g., through massive open online courses)^{xliv} and possible outreach. To illustrate, AI micro-certifications, or micro-credentials^{xlv} (these terms are used interchangeably) can be a crucial tool to facilitate matching on the labour market, and to allow skill endowment to be more accurately assessed and recognised by the industry.^{xlvi} Considering the global trend, institutions and universities in India may consider similar approaches and redesign the AI/ML courses or programs currently being offered.

Section 5.11. Accreditation

Q34. 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 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.

Section 5.12. Procurement of AI Solutions or Products

Q35. Whether creating a framework to prepare a list of prequalified suppliers of AI products or solutions will help industry including government agencies to procure AI products or solutions? Whether there is a need to formulate a standard Code of Conduct or guidelines for AI related procurements? What should be the typical elements of such a Code of Conduct or guidelines including guidelines on trusted source and who should be tasked to formulate such a Code of Conduct or guidelines? Please justify your response with rationale and suitable examples, if any.

Response:

It may be premature to create a list of prequalified suppliers, or creating a system for accreditation, of AI products or solutions. Such an approach may be counter-productive to the evolving AI ecosystem in India by creating entry barriers for start-ups and innovators to participate in the markets for such products and solutions. Instead, we suggest that the TRAI look to analyse, more generally, on the responsible use of AI in the public sector. Various government bodies have already started deploying AI products and solutions in India. There is merit in exploring how to ensure accountability vis-à-vis unique risks and concerns posed by such deployments in the public sector, since such deployments can uniquely interfere with fundamental rights and public law.^{xlvii} The Paper mentions that some guidelines may be required to have a standard code of conduct for adoption. We are unclear of what such a code may contain and request clarity in this regard.

Section 5.13. Compendium of Toolkits and Use Cases

Q36. 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.

Section 5.14. Establish Centre for Excellence

Q37. 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 TCoEs? Please justify your response with rationale and global best practices, if any.

Q38. 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.

Q39. Any other issue which is relevant to this subject? Please suggest with justification.

Response:

Building a compendium of best practices

We agree, in principle, with the need to build toolkits to help in analysing use-cases related to AI & BD to foster adoption in the telecom sector. This would be useful to proliferate best practice and in better preparing for the risk assessment exercise suggested above. We would be happy to work with the TRAI in this regard – given the extensive already undertaken by NASSCOM in this regard. Specifically, NASSCOM has, as part of a joint venture with the Central Government, established the INDIAai (the National AI Portal of India and also cited in the Paper), which is intended to serve as a single knowledge hub on AI and allied fields.^{xlviii} NASSCOM has also recently published a compendium of use-cases called 75@75 – India’s AI Journey.^{xlx} Given this pre-existing expertise and experience, we suggest that specific work for the telecom sector can be undertaken as a continuation of the ongoing efforts being undertaken by INDIAai, so as to build a consolidated cross-sectoral pool of AI toolkits and use cases.

Establishing centres of excellence

We agree, in principle, on the need to build collaborations between governments, industry and academia to bolster the local ecosystem and build local talent. Industrial nations have generally leveraged industry-university partnerships to enable industrial growth and change.^l We also encourage government bodies to invite public-private partnerships to accelerate AI adoption.

However, on establishing new Centres of Excellence (COEs) or linkages between telecom industry & academia, we suggest that the TRAI may look to first map out existing Centres of Excellence on AI & BD set up by the private or public sector and identify opportunities for deepening linkages between them and other stakeholders. One example of such a market driven COEs on AI & BD include the COE between Indian Institute of Sciences in Bengaluru and Nokia,

which is to promote interdisciplinary research involving emerging technologies like AI, robotics, and advanced communication technologies like 5G.^{li} An example of such a COE set up a government body is that set up by the National Informatics Centre.^{lii} NASSCOM has also set up a centre of excellence for IOT and AI in 2021, fostering a partnership between industry and both the Central Government and four State Governments.^{liii} We suggest that the TRAI explore on how to build on such existing efforts and fostering more collaborations between them.

Similarly, on skill development, we note that industry-academia linkages do already exist, and opportunities for deepening them may be explored. For example, IIT Bombay is part of IBM's "AI Horizons Network", an international consortium of leading universities around the world, which included MIT, University of Michigan, University of Maryland among others, working with IBM to develop AI related capabilities.^{liv} We would be happy to work with the TRAI in this regard.

Please note that, in this response, we offer the above examples citing specific members merely as illustrations and not as endorsements of initiatives taken by specific members over others.

For any queries related to this submission, please contact:

- **At NASSCOM:** Ashish Aggarwal (asaggarwal@nasscom.in), Vertika Misra (vertika@nasscom.in), Varun Sen Bahl (varun@nasscom.in) or Sudipto Banerjee (sudipto@nasscom.in).
- **At DSCI:** Vinayak Godse (Vinayak.Godse@dsci.in), Deepa Ojha (deepa.ojha@dsci.in), or Anisha Koshy (anisha@dsci.in).

About NASSCOM

The National Association of Software and Services Companies (**NASSCOM**) is the premier trade body and chamber of commerce of the Tech industry in India and comprises over 3000 member companies including both Indian and multinational organisations that have a presence in India. Established in 1988, NASSCOM helps the technology products and services industry in India to be trustworthy and innovative across the globe. Our membership spans across the entire spectrum of the industry from start-ups to multinationals and from products to services, Global Service Centres to Engineering firms. Guided by India's vision to become a leading digital economy globally, NASSCOM focuses on accelerating the pace of transformation of the industry to emerge as the preferred enablers for global digital transformation. For more details, kindly visit www.nasscom.in

About DSCI

The Data Security Council of India (**DSCI**) is a premier industry body on data protection in India, setup by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI brings together governments and their agencies, industry sectors including ITBPM, BFSI, telecom, industry associations, data protection authorities and think-tanks for policy advocacy, thought leadership, capacity building and outreach initiatives. For more info, please visit www.dsci.in

Endnotes

- ⁱ Telecom Regulatory Authority of India, [Consultation Paper on Leveraging Artificial Intelligence and Big Data in Telecommunication Sector](#), (August 2022).
- ⁱⁱ Specifically, the DOT sought recommendations on how to leverage BD and AI in “a synchronized and effective manner to enhance the overall quality of service, spectrum management, network security and reliability”, citing the relevant clause in the National Digital Communications Policy of 2018. See, Annexure I, page 159, the Paper.
- ⁱⁱⁱ Specifically, the DOT sought recommendations on how to leverage BD and AI in “a synchronized and effective manner to enhance the overall quality of service, spectrum management, network security and reliability”, citing the relevant clause in the National Digital Communications Policy of 2018. See, Annexure I, page 159, the Paper.
- ^{iv} The Paper states: “The aspects of AI and BD referred by the DoT for seeking recommendations from TRAI mainly focusses on the telecom sector. However, there are many other sectors where telecom and Information and Communications Technology (ICT) sector can play an important role in building AI based capacity and capabilities.” See, Section 1.3.1 of the Paper.
- ^v See Future of Privacy Forum, [the Spectrum of Artificial Intelligence](#), (2021).
- ^{vi} See, European Parliament, [Understanding algorithmic decision-making: opportunities and challenges](#), (2019)
- ^{vii} See D. Montoya, A. Rummery, [The use of artificial intelligence by government: parliamentary and legal issues](#), New South Wales Parliamentary Research Service, (2020).
- ^{viii} See, Stone et. al., [Artificial Intelligence and Life in 2030: Report of 2015 Study Panel of the One Hundred Year Study on Artificial Intelligence](#), Stanford University, (September 2016).
- ^{ix} See, P. Saxena, [Levels of autonomy in autonomous vehicles](#), IndiaAI, (2021).
- ^x See, J. Schuett, [Defining the scope of AI regulations](#), the Legal Priorities Project, (2021).
- ^{xi} See, Stanford University, [Artificial Intelligence and Life in 2030 - One Hundred Year Study on Artificial Intelligence](#), (2016).
- ^{xii} See, Matt O’Shaughnessy, [One of the Biggest Problems in Regulating AI Is Agreeing on a Definition](#), Carnegie Endowment for International Peace, (2022)
- ^{xiii} See, Michael Gaynor, [Automation and AI sound similar, but may have vastly different impacts on the future of work](#), Brookings, (2020).
- ^{xiv} See, Future, [The New Business of AI \(and How It’s Different From Traditional Software\)](#), (2020).
- ^{xv} See, UNESCO, [Recommendation on the Ethics of Artificial Intelligence](#), (2022). Also, see, UNESCO, Press Release, [UNESCO member states adopt the first ever global agreement on the Ethics of Artificial Intelligence](#), (November 25, 2021).
- ^{xvi} See, UNESCO, [Recommendation on the Ethics of Artificial Intelligence](#), (2022).
- ^{xvii} See, A. Jobin et. al., [Artificial intelligence: the global landscape of ethics guidelines](#), ETH Zurich, (2019).
- ^{xviii} For an example of such a thematic mapping exercise, see, J. Fjeld, et. al., [Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI](#), Berkman Klein Centre for Internet & Society, (2020); A. Jobin et. al., [Artificial intelligence: the global landscape of ethics guidelines](#), ETH Zurich, (2019).
- ^{xix} See, NASSCOM RAI Kit.
- ^{xx} See, IndiaAI, [AI is being used to improve operational efficiency and service quality](#), (2019).
- ^{xxi} See, NASSCOM, [AI Patents – Driving Emergence of India as an AI Innovation Hub](#), (2021).
- ^{xxii} See, NASSCOM, [AI Gamechangers 2022: Realising India’s AI promise](#), (2022).
- ^{xxiii} See, NASSCOM, [AI Platforms – Next Frontier for Indian IT Services](#), (2020).
- ^{xxiv} For a discussion on the privacy risks posed by big data in telecom, FIGI, [Big data, machine learning, consumer protection and privacy](#), International Telecommunications Union, (2020).
- ^{xxv} AI Multiple, [Top 10 Privacy Enhancing Technologies \(PETs\) & Use Cases](#)
- ^{xxvi} See, V. Ramdas, P. Mishra, N. Jain, A. Chaturvedi, [Handbook on Data Protection and Privacy for Developers of Artificial Intelligence \(AI\) in India: Practical Guidelines for Responsible Development of AI](#), DSCI, Digital India Foundation, Koan Advisory, FAIR Forward, GIZ India, German Federal Ministry for Economic Cooperation and Development, (2021).
- ^{xxvii} See, Germany, [Opinion of Data Ethics Commission](#), (2019).
- ^{xxviii} Some of these laws are - Indian Telegraph Act, 1885 (the new Draft Indian Telecommunication Bill, 2022 proposes to repeal this legislation); Information Technology Act, 2000; Indian Penal Code, 1860; Copyright Act, 1957; Patent Act, 1970; Competition Act, 2002; and Consumer Protection Act, 2019.
- ^{xxix} See, NASSCOM, [Responsible AI Architects Guide](#), (2022).
- ^{xxx} See, Department of Telecommunications, [Indian Artificial Intelligence Stack](#), (September 02, 2020).
- ^{xxxi} See, NASSCOM, [Feedback on the Discussion Paper on Indian AI stack](#), (November 03, 2020).
- ^{xxxii} See, NASSCOM, [Unlocking Value from Data and AI: the India Opportunity](#), (2020).
- ^{xxxiii} See, NASSCOM, [Responsible AI: resource kit](#), (2022) (NASSCOM RAI Kit).
- ^{xxxiv} See, NASSCOM, [AI-as-a-service: democratizing AI for scale](#), (2022).
- ^{xxxv} See, UNESCO, [Recommendation on the Ethics of Artificial Intelligence](#), (2022).
- ^{xxxvi} See, NASSCOM, [Unlocking Potential of India’s Open Data](#), (2022).
- ^{xxxvii} See, NASSCOM, [Talent Demand & Supply Report: AI & Big Data Analytics](#), (2018).
- ^{xxxviii} See, NASSCOM, [Responsible AI Architects Guide](#), (2022).
- ^{xxxix} See, World Economic Forum, [The Global Gender Gap Report](#), (2018).
- ^{xl} See, NASSCOM, [Feedback on the draft India Data Accessibility and Use Policy](#), (2022); NASSCOM-DSCI, [Feedback on the draft National Data Governance Framework Policy](#), (2022).

-
- ^{xli} See, Sections 22-24 of the [Draft Payment and Settlements Bill, 2018](#).
- ^{xlii} See, Vidhi Centre for Legal Policy, [Blueprint of a Fintech Regulatory Sandbox Law - Preparing for the Future of Fintech Innovations](#), (March, 2020). This concept paper envisages a legal framework for sandboxing in India that will be instrumental in defining the future of fintech innovations in India.
- ^{xliii} See, [OECD Education Policy Perspectives: Micro-Credential innovations in higher education: Who, What and Why ?](#) (September 22, 2021).
- ^{xliv} See, [Massive Open Online Courses](#).
- ^{xlv} See, Milligan and Kennedy, [To What Degree? Alternative Micro-Credential in a Digital Age](#), (Chapter 4, page 40) of Visions for Australian Tertiary Education (2017). As the name implies, **micro-credentials** focus on modules of learning (like, 'nano-degrees', 'micro-masters', 'credentials', 'certificates', 'badges', 'licenses' and 'endorsements') much smaller than those covered in conventional academic awards, which often allow learners to complete the requisite work over a shorter period." As their name implies, micro-credentials focus on modules of learning much smaller than those covered in conventional academic awards, which often allow learners to complete the requisite work over a shorter period. In their most developed form, micro-credentials represent more than mere recognition of smaller modules of learning. They form part of a digital credentialing ecosystem, made possible by digital communications technologies establishing networks of interest through which people can share information about what a learner knows and can do. For example, University of Florida provides [micro-certification](#) to learners on key concepts and foundational knowledge for understanding AI Modules and it covers both technical and ethical aspects of AI. [Microsoft Certified: Azure AI Fundamentals](#) and Microsoft [Digital Literacy Certification](#) aims to help individuals prove they have the skills needed for AI jobs, including in relation to machine learning, responsible AI, computer vision and NLP.
- ^{xlvi} See, Borhene and Keevy, UNESCO, [Digital Credentialing: implications for the recognition of learning across borders](#), (2018).
- ^{xlvii} For a general discussion on the issues of algorithmic accountability in the public sector, see, Ada Lovelace Institute, AI Now Institute and Open Government Partnership, [Algorithmic Accountability for the Public Sector](#), (2021).
- ^{xlviii} See [INDIAai](#).
- ^{xlix} See NASSCOM, [75@75 – India's AI Journey](#), (2022).
- ⁱ See, ICRIER, [Implications of AI on the Indian Economy](#), NASSCOM & Google, (2020).
- ⁱⁱ See, Nokia, [Nokia partners with Indian Institute of Science to establish Networked Robotics Center of Excellence](#), (2022).
- ⁱⁱⁱ See, National Informatics Centre: <https://www.nic.in/emergings/centre-of-excellence-for-artificial-intelligence/>
- ⁱⁱⁱⁱ See, NASSCOM, [K-Tech COE on Data Science and Artificial Intelligence](#), (2021); NASSCOM, [COE on IOT](#), (2021).
- ^{iv} See, IBM, [IBM and IIT Bombay team up to accelerate AI research in India](#), (2018).