TRAI Consultation Paper

on

“Digital Transformation through 5G Ecosystem”

Nokia response

We thank the Telecom Regulatory Authority of India (TRAI) for providing us with the opportunity to share the response to the Consultation paper on **“Digital Transformation through 5G Ecosystem.”**

In today's interconnected world, digital technology has become synonymous with opportunity, shaping education, healthcare, employment, and civic engagement. Unparalleled technological advancement will shape life as we know it in the upcoming decade.

By 2030, the world will have undergone a significant transformation. The global rate of technology adoption will be impacted by trends such as a deepening focus on environmental sustainability, cybersecurity, and inclusion. Advances in semiconductors, software, artificial intelligence (AI) and machine learning (ML), digital twins, metaverse technologies, Web3 and cloud technologies will continue to accelerate.

Over the next decade, technology will continue to significantly extend the scope of human possibilities, connecting the human, physical and digital worlds. The human world will be the driving source of technology innovation thanks to our irreplaceable capacity for perception, emotion, logic, intent, culture, and aspiration. The advancing digital world is powered by increasingly complex and disruptive technologies, which it utilizes to supervise and automate the tangible objects of the physical world. The convergence of these worlds will transform societies, governments and businesses enabling us to reach our full potential.

The 5G ecosystem requires significant investment in infrastructure development, a collaborative regulatory environment, Collaboration between Academia, start-ups and industry verticals for research & development, testing and deployment of relevant use cases. Our Society needs to be committed enough to overcoming the digital divide to ensure equitable access and benefits for all.

In consideration of above, please find below our response on the consultation paper.

Q.1. Is there a need for additional measures to further strengthen the cross-sector collaboration for development and adoption of 5G use cases in India? If answer is yes, please submit your suggestions with reasons and justifications. Please also provide the best practices and lessons learnt from other countries and India to support your comments.

Nokia Response:

Establish a National 5G Task Force: Include representatives from key sectors like healthcare, education, and manufacturing. A dedicated task force will ensure that all sectors are aligned in their approach towards adopting and leveraging 5G. It facilitates the sharing of insights, resources, and best practices, ensuring that 5G implementation is efficient and cohesive across various industries. It also helps in accelerating nationwide 5G rollout, ensuring uniform adoption across sectors, and fostering innovation through collaborative efforts.

Host Regular Innovation Summits: Facilitate collaboration and idea-sharing between industries - Innovation summits bring together leaders from various industries, academia, and government, fostering a collaborative environment. They serve as platforms for discussing challenges, sharing ideas, and showcasing new technologies. They also promote knowledge exchange, encourages joint ventures, and helps in identifying and solving sector-specific challenges with 5G.

- ➢ Finland's 5G Momentum ecosystem encourages collaboration through regular events and workshops, bringing together various stakeholders. 5G Momentum ecosystem makes Finland a pioneer in 5G | Traficom Finland working in international cooperation towards future technologies - FiCom

Q.2. Do you anticipate any barriers in development of ecosystem for 5G use cases, which need to be addressed? If yes, please identify those barriers and suggest the possible policy and regulatory interventions including incentives to overcome such barriers. Please also provide the details of the measures taken by other countries to remove such barriers. [2.63]

Nokia Response:

- **Barrier - Infrastructure Challenges:** One of the primary obstacles in the rollout of 5G is the lack of adequate infrastructure, Labs, particularly in rural and remote areas and lack of Monetization opportunity for CSP. This includes insufficient cell towers, fiber optic lines, and other necessary hardware. CSP may be incentivized for rollout in some manner as they are not getting return of investments.

- **Policy Intervention - Infrastructure Development Grants:** Infrastructural development is crucial for 5G deployment. Grants can stimulate investment in necessary hardware, such as cell towers and fiber optics, especially in rural and underserved areas. Encourage development in regions that may not be immediately profitable for private companies.
    - ➢ The U.S. Federal Communications Commission's (FCC) Rural Digital Opportunity Fund allocates funds to build and maintain infrastructure. Auction 904: Rural Digital Opportunity Fund | Federal Communications Commission (fcc.gov)
- **Barrier - Spectrum Accessibility and Utilization**: Efficient and strategic spectrum management is crucial for 5G networks. The barrier here is not only the availability of spectrum but also its optimal allocation and pricing. Reforms in spectrum management can ensure fair and efficient use of this resource.

Q.3. What are the policy measures required to create awareness and promote use of 5G technology and its infrastructure so that the citizens including those residing in rural and remote areas may benefit from the 5G use cases and services to create new economic activities and increase employment opportunities and thereby promote economic growth of the country? [2.64]

Nokia Response:

- **Nationwide Digital Literacy Campaigns**: A major barrier to 5G adoption is the lack of awareness and understanding of its benefits and applications, especially in rural and remote areas. Educate citizens about the benefits and uses of 5G by running literacy campaigns tailored around 5G & its application benefits. Customize campaigns to address specific regional needs and language barriers. Use a mix of traditional and digital media to reach a wider audience.
    - ➢ Singapore's Smart Nation initiative focuses on increasing digital literacy and public awareness of new technologies. Transforming SG Through Tech (smartnation.gov.sg)
    - ➢ Australia's Regional Tech Hub is another example. Regional Tech Hub improving digital literacy for rural Australians – Rowan Ramsey MP
- **Subsidize 5G-Enabled Devices**: The high cost of 5G-enabled devices and services can be prohibitive, especially in underprivileged, lower-income and rural areas.

Partner with device manufacturers to offer discounted 5G smartphones and gadgets. Implement subsidy schemes or provide affordable pricing models for 5G services.

- **Educational Programs and Training Workshops**: There is a need to educate not just the public but also businesses and local governments about the potential applications and benefits of 5G. Host workshops and training programs for small businesses and local government officials. Develop online resources and training modules accessible nationwide.
  - ➢ **Finland's 5G MOOC** (Massive Open Online Course) provides comprehensive knowledge about 5G technology to a broad audience. 5G MOOC - MOOC.fi courses

Q.4. What are the policy measures required to promote use of IoT technology and its infrastructure so that the citizens including those residing in rural and remote areas may benefit from these 5G enabled IoT smart applications and services to create new economic activities and increase employment opportunities and thereby promote 159 economic growths of the country? [3.26]

Nokia Response:

- **Develop IoT Innovation Hubs:** Innovation hubs can serve as centers for developing and testing IoT solutions tailored to local needs, fostering technological advancement in rural areas. Innovation hubs could also facilitate partnerships between local governments, educational institutions, and private companies along with supporting incubation services, technical support, and funding for IoT startups focusing on rural challenges.
  - ➢ **Germany's Digital Hub** Initiative promotes digital innovation across various regions, with a focus on different technological sectors. Welcome | de:hub digital ecosystems (de-hub.de)
- **Financial Incentives for IoT Startups:** Startups are often at the forefront of IoT innovation. Financial incentives can stimulate growth and development of new IoT solutions & encourage local IoT solution development. Offer tax breaks, grants, and subsidized loans for IoT startups. Create competitive funding opportunities for IoT projects with societal impact.

   - ➢ The **European Union's Horizon 2020** program offered funding for research and innovation projects, including several IoT. It has been a highly successful program with broad impact across Industries. EU Horizon 2020 IoT

- **Subsidizing IoT Devices for Consumers and Businesses:** The high cost of IoT devices can be a barrier to adoption, especially for small businesses and consumers in rural areas. Implement schemes to reduce the cost of IoT devices for small and medium-sized enterprises (SMEs) and agricultural applications. Provide rebates or vouchers for IoT home devices to encourage consumer adoption.

   - ➢ **Japan's Society 5.0** initiative includes subsidies for IoT adoption in various sectors, including agriculture. Society 5.0 (cao.go.jp)

Q.5. What initiatives are required to be taken by the Government to spread awareness among the citizens about IoT enabled smart applications? Should the private companies / startups developing these applications need to be engaged in this exercise through some incentivization schemes? [3.27]

Nokia Response:

- **Incentivizing Private Companies for Developing Localized IoT Applications**: Localized IoT applications tailored to specific regional needs can be more effective in demonstrating the practical benefits of IoT. Offer tax incentives or grants to companies that develop IoT solutions addressing local challenges. Facilitate public-private partnerships for community-specific IoT projects.
   - ➢ In Singapore, the government collaborates with private companies to develop smart city solutions, a model that can be adapted for rural IoT applications. Smart Nation Singapore

- **Collaborating with Educational Institutions:** Educational institutions can play a crucial role in disseminating knowledge about IoT technologies. Integrate IoT-related subjects and practical projects into school and college curricula. Organize workshops and seminars in collaboration with tech companies and experts.

   - ➢ The MIT Media Lab runs various programs and workshops on emerging technologies like IoT, serving as a model for educational collaboration. MIT Media Lab

- **Policy Framework for IoT Integration in Government Services**: Integrating IoT into government services can improve their efficiency and accessibility, serving as a powerful example of IoT's benefits. Develop government programs that utilize IoT for public services like waste management, water quality monitoring, etc. Publicize successful implementations to increase public trust in IoT technology.

- **Barcelona's Smart City** project utilizes IoT for various urban services, demonstrating effective public-sector IoT integration. Barcelona Smart City

Q.6. Industry 4.0 encompasses Artificial intelligence, Robotics, Big data, and the Internet of things and set to change the nature of jobs.

(a) **What measures would you suggest for upskilling the top management and owners of industries?**

Nokia Response:

(a) - Top management needs to understand the strategic implications of Industry 4.0 to drive change within their organizations. Conduct executive education programs focusing on digital transformation and Industry 4.0. Partner with leading business schools and tech firms to offer customized workshops. Stanford University offers executive education programs in digital business strategy that could serve as a model. Similar programs could be established with support from Indian academia & institutes like the IIMs & other management schools. The Innovative Technology Leader | Stanford Graduate School of Business

- **(b) What measures would you suggest for upskilling the workforce of industries?**

Nokia Response:

(b)- The workforce needs new skills to operate and thrive in an Industry 4.0 environment, such as data analytics, IoT management, and cybersecurity. Develop technical training programs in partnership with industry players. Offer online courses and certifications to make training accessible.

- ➢ Siemens' partnership with various educational institutions to provide digital skills training. Similar programs could be built with support from Indian / Global Tech companies Siemens SCE - Education & Learning - Siemens Global Website

- **(c) What kind of public private partnership models can be adopted for this upskilling task? Please reply with proper justification and reasons and also by referring to the global best practices in this regard. [3.29]**

  Nokia Response:

  (c)- PPP models can leverage the strengths and resources of both the public and private sectors for effective skill development. Government can provide funding and policy support, while private entities offer technological expertise and training resources.Focus on creating sector-specific training centres.

  ➢ **SkillsFuture Singapore** is a PPP initiative aimed at lifelong learning and skills development Home (skillsfuture.gov.sg)

Q.7. What are the policy, regulatory and other challenges faced by MSMEs in India in adoption of Industry 4.0. Kindly suggest measures to address these challenges. Provide detailed justification with reasons along with the best practices in other countries. [3.41]

Q.8. What additional measures are required to strengthen the National Trust Centre (NTC) framework for complete security testing and certification of IoT devices (hardware as well as software) under DoT / TEC. What modifications in roles and responsibilities are required to make NTC more effective? Kindly provide your comments with justification in line with the global best practices

Nokia Response:

By strengthening the NTC's framework and aligning its roles and responsibilities with international best practices, India can ensure a secure and trusted environment for IoT and related technologies. This is crucial not only for domestic security but also for the global competitiveness of Indian IoT products and services.

- **Additional measures required to strengthen the National Trust Centre (NTC) framework-** As IoT devices increasingly permeate critical sectors like healthcare, finance, and infrastructure, ensuring their security is paramount. The National Trust Centre (NTC) needs to be equipped to rigorously test and certify these devices for robust security standards.

- **Policy Interventions**
  - Expand NTC's capabilities to include a wider range of IoT devices and software, covering various industry verticals.
  - Adopt international security standards and practices to ensure global competitiveness and interoperability.
- **International Best Practice** - The European Union's Cybersecurity Certification Framework under the Cybersecurity Act provides a comprehensive approach to certifying the security of ICT products, which could serve as a model. Cybersecurity Certification (europa.eu)

- **Modifications in Roles and Responsibilities for Enhanced Effectiveness**: As technology evolves, the roles and responsibilities of the NTC must also adapt to address emerging threats and challenges effectively.
  - **Policy Interventions**
    - Introduce specialized departments within the NTC focusing on different aspects of IoT security, such as hardware, software, and data protection.
    - Foster collaboration with international cybersecurity organizations to stay updated with global best practices and threat intelligence.
  - **International Best Practice**: The National Cybersecurity Centre in the UK plays a proactive role in cybersecurity across various sectors, offering a potential model for the NTC's evolving role. UK National Cybersecurity Centre
- **Incorporating Global Best Practices into the NTC's Framework**: Aligning with global best practices not only enhances the NTC's effectiveness but also ensures that Indian IoT products are trusted and accepted worldwide.
  - **Policy Interventions**
    - Regularly update certification processes based on international standards like ISO/IEC 27001.
    - Engage in international forums and bilateral agreements to align security standards and practices.

- **International Best Practice**: Singapore's Cybersecurity Strategy involves active international collaboration and alignment with global standards, making it a relevant model for the NTC. The Singapore Cybersecurity Strategy 2021 (csa.gov.sg)

Q.9. IoT security challenges and requirements vary significantly across different industry verticals. Is there a need to develop sector specific IoT security and privacy guidelines?

Nokia Response:

The development of sector specific IoT security and privacy guidelines, underpinned by a common framework, is essential to address the diverse and complex challenges posed by IoT across different industry sectors. By doing so, not only is the integrity and security of IoT systems upheld, but also their interoperability and compliance with broader regulatory standards are ensured. This dual approach allows for the tailored protection of sector-specific needs while maintaining a consistent security posture across the IoT landscape.

- **Need for Sector-Specific IoT Security Guidelines**: Different industry sectors have unique security challenges and requirements for IoT. For instance, healthcare IoT devices demand stringent data privacy measures, while industrial IoT requires robust protection against operational disruptions.
    - **Policy Interventions:**
        - Tailor security protocols to address specific threats in sectors like healthcare, manufacturing, agriculture, and smart cities.
        - Incorporate industry-specific compliance standards into IoT security guidelines.
- **International Best Practice:** The Health Insurance Portability and Accountability Act (HIPAA) in the U.S. provides specific guidelines for protecting sensitive patient data, a model that can be adapted for healthcare IoT. HIPAA Guidelines
- **Developing a Common Framework for Guideline Creation**: While sector-specific guidelines are necessary, a common framework ensures consistency and interoperability across different IoT applications.

- **Policy Interventions**:
  - Establish a baseline of security standards applicable to all IoT devices, regardless of the sector.
  - Create a regulatory body to oversee the adaptation of these standards into sector-specific guidelines.

Q.10. If answer to Q.9 is yes, is there a need for a common framework and methodology for developing such sector-specific guidelines.

Nokia Response:

A common framework for developing sector specific IoT security guidelines ensures that the fundamental aspects of IoT security are uniformly addressed, while also providing the flexibility to cater to the unique requirements of different industries. This approach facilitates easier management, regulation, and enforcement of IoT security standards, contributing to a safer and more secure IoT ecosystem.

- **Establishing a Unified Framework for IoT Security**: A common framework for IoT security ensures consistency and interoperability across different sectors, making it easier to manage and regulate IoT security on a national scale.

  - **Policy Interventions:**
    - The framework should include core security principles like data encryption, user authentication, and regular security updates, applicable to all IoT devices.
    - Align with Global practice to avoid any delay in rolling out technology in India.

  - **Methodology for Tailoring Sector-Specific Guidelines:** Different industries have unique security and operational requirements. A common methodology ensures that these specific needs are systematically addressed while maintaining a baseline security standard.

  - **Policy Interventions:**
    - The methodology should include risk assessment procedures, compliance checks, and best practices for each sector.
    - Regular consultations with industry experts and stakeholders to keep the guidelines relevant and up to date.

- **International Best Practice**: The European Union's General Data Protection Regulation (GDPR) provides a broad framework for data protection that can be adapted for specific sectors. [General Data Protection Regulation (GDPR) Compliance Guidelines]

- **Role of Government and Industry in Framework Development**: Collaboration between government and industry stakeholders is crucial for creating a balanced and effective IoT security framework.
    - Policy Interventions:
        - Establish a joint task force with representatives from government, industry, academia, and consumer groups.
        - Utilize public feedback and pilot testing in different sectors to refine the framework.
    - **International Best Practice**: Singapore's multi-stakeholder approach in developing its Smart Nation plan, which includes IoT security measures. Smart Nation Singapore

Q.11. Please suggest regulatory and policy interventions required to ensure privacy of the massive amount of sensitive user data generated by IoT applications specifically in light of the Digital Personal Data Protection Act, 2023. Kindly provide justifications along with the global best practices.

Nokia Response:

Ensuring the privacy of IoT user data is critical in the age of connected devices. By implementing regulatory and policy interventions, aligning with existing data protection laws, and adopting industry best practices, India can create a secure and trustworthy IoT ecosystem. This approach not only protects individual privacy rights but also fosters consumer confidence in IoT technologies, essential for their widespread adoption and success.

- **Regulatory and Policy Interventions for IoT Data Privacy**: The massive amount of sensitive user data generated by IoT applications poses significant privacy risks, making regulatory interventions crucial to protect individual rights and maintain public trust.

    ➢ **Policy Interventions**:

        - Develop comprehensive data protection regulations specific to IoT, addressing data collection, storage, processing, and sharing.

        - Implement mandatory data breach notification requirements for IoT service providers.

    - **International Best Practice**: The EU's General Data Protection Regulation (GDPR) provides robust data privacy protections that can be adapted for IoT contexts. General Data Protection Regulation (GDPR) Compliance Guidelines

- **Alignment with Digital Personal Data Protection Act 2023**: Aligning IoT data privacy measures with the Digital Personal Data Protection Act 2023 ensures consistency in data protection laws and helps avoid regulatory overlaps.

    - **Policy Interventions**:

        - Clarify the application of the Digital Personal Data Protection Act 2023 in the context of IoT, especially for data minimization and user consent.

        - Regularly update the legal framework to keep pace with IoT technological advancements.

- **International Best Practice**: The California Consumer Privacy Act (CCPA) in the U.S. is an example of legislation that addresses digital data privacy comprehensively. California Consumer Privacy Act (CCPA)

- **Best Practices for IoT Data Management**: Establishing best practices for IoT data management can guide organizations in implementing effective privacy measures.

    - **Policy Interventions**:

        - Promote the adoption of privacy by design principles in IoT development.

        - Encourage transparency in IoT data practices, including clear user privacy policies.

- **International Best Practice**: The IoT Security Foundation provides a set of best practices for IoT privacy and security. IoT Security Foundation Best Practices

Q.12. What additional policy and regulatory measures are required to encourage research and development of IoT use cases in various sectors? Is there a need to incentivize startups for research and development of IoT enabled use cases in various industry verticals? If yes, kindly suggest measures for the same.

&

Q.13. What measures should be taken to encourage centres of excellence to handhold startups working in the development of use cases and applications in 5G and beyond technologies? How can the domestic and foreign investors be encouraged to invest for funding the startups for these kinds of development activities? [3.79]

Nokia Response:

5G needs to be capitalized for Industry 4.0 proliferation in the Country. Various Industry verticals wish to enhance their productivity, efficiency and have sustainable growth. Industry verticals are looking for such uses cases for their Operational requirements be it in IOT, CLOUD, Digital twin AR VR etc. To increase the research and development in these respective domains, collaboration needs to be emphasized between Industry, Academia, start-ups, and technology solution providers. 5G ecosystem players involved in such center of excellence needs to be incentivized. Industry vertical adopting the industry 4.0 initiative needs to be incentivized. Encouragement for Devices ecosystem players with lower taxes & duties for few initial years will help in adoption of 5G and IOT applications in various industry verticals.

Q.14. Whether there is a need to make changes in relevant laws to handle various issues, including liability regime and effective mechanism for redressal and compensation in case of accidents, damages, or malfunctions involving IoT, drones, or robotic systems. If yes, give detailed suggestions. 161 [3.81]

Q.15. Is there a need to have a separate security mechanism for Multiaccess Edge Computing (MEC)? If yes, please give your inputs and suggestions with regard to policies, rules, regulations and guidelines.

Nokia Response:

Establishing a comprehensive security mechanism for Multi-access Edge Computing is essential in the evolving landscape of 5G and IoT. It requires a blend of specialized security protocols, robust policy frameworks, and multi-stakeholder collaboration to address the unique security demands of edge computing. By adopting these measures, India can ensure the secure and resilient deployment of MEC, a critical component in the next generation of wireless technology infrastructure.

- **Need for a Separate Security Mechanism in MEC:** Multi-access Edge Computing (MEC) introduces unique security challenges due to its decentralized nature and proximity to users. A specialized security mechanism is crucial to protect against threats like data breaches, unauthorized access, and cyber-attacks at the network edge.

    - **Policy Interventions:**

        - Develop security protocols tailored to the edge environment, considering the higher risk of physical access and the need for rapid data processing.

        - Implement robust encryption and authentication measures to secure data transmission between edge devices and central networks.

    - **International Best Practice: The ETSI whitepaper on MEC security outlines various security considerations and recommendations.** White Paper on MEC security (etsi.org)

- **Policy, Rules, and Regulation Suggestions for MEC Security:** Establishing clear policies, rules, and regulations is vital to standardize and enforce security practices across MEC implementations.

    - **Policy Interventions:**

        - Define compliance standards for MEC providers, including requirements for regular security audits and vulnerability assessments.

        - Set guidelines for data localization and processing at the edge, keeping in mind privacy laws and regulations.

    - **International Best Practice:** The European Telecommunications Standards Institute (ETSI) has developed standards for MEC that include security aspects. **ETSI MEC Standards**

- **Collaboration with Industry and International Bodies:** Collaborating with industry stakeholders and international bodies ensures that MEC security mechanisms are up-to-date with global standards and best practices.
  - **Policy Interventions:**
    - Engage in partnerships with global tech companies and cybersecurity experts to share knowledge and resources.
    - Actively participate in international forums to align MEC security standards with global norms.

Q.16. What are the policy measures required to create awareness and promote use of Metaverse, so that the citizens including those residing in rural and remote areas may benefit from the Metaverse use cases and services to create new economic activities and increase employment opportunities and thereby promote economic growth of the country?

Nokia Response:

Ubiquitous usage of Metaverse requires a) awareness of Metaverse use cases and services b) access to Metaverse technology: connectivity and devices c) the technology skills to safely and confidently make use of Metaverse services, and to create Metaverse services.

Regional Metaverse hubs can contribute to these goals by:

- Organizing demonstration sessions of devices and services with fixed and mobile set-ups, for educational institutions, enterprises and the public sector, tuned to the audience.
- Create educational packages for students and citizens, helping them to safely and confidently use Metaverse services, and contribute to Metaverse experiences through the creation of information and 3D content
- Collaborate with educational institutions and sectorial organizations to develop educational curricula for Metaverse skill development: ICT Metaverse specialists and Metaverse content creators.

Examples of international best practices

- European Digital Innovation Hubs
- Metaverse skill development in the frame of the Digital Europe Programme, Section 4.1 Specialized Education Programmes in Key Capacity Areas.

- The planned EU action to develop a Virtual Worlds Toolbox for the general public, in An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition, p.8

Q.17. Whether there is a need to develop a regulatory framework for the responsible development and use of Metaverse? If yes, kindly suggest how this framework will address the following issues:
i. How can users control their personal information and identity in the metaverse?
ii. How can users protect themselves from cyberattacks, harassment and manipulation in the metaverse?
iii. How can users trust the content and services they access in the metaverse?
iv. How can data privacy and security be ensured in the metaverse, especially when users may have multiple digital identities and avatars across different platforms and jurisdictions?

Nokia Response:

Due to the novel immersive modality of the Metaverse, it can be expected that novel challenges around privacy, identity, harassment, trust and security will emerge that go beyond those of current online services. At the same, the Metaverse is currently in a very early stage and will take a decade or more to mature, in directions that are difficult to imagine. A sound regulatory basis that protects users in established online services like social media, search, ecommerce sites and applications, gaming etc. is the best basis to tackle future Metaverse challenges around privacy, identity, harassment, trust and security, as the main protectory mechanisms will also apply to emerging Metaverse services. It is recommended to closely monitor the development of Metaverse platforms and services, verify if the regulation in place covers the emerging Metaverse services operation and usage, and take regulatory action when required. It is furthermore recommended to align new regulatory action on a global scale.

Examples of international best practices

- The EU has decided in An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition, not to develop Metaverse-specific regulation for the moment, deeming that the current legislative framework is robust and future-oriented, with the Digital Services Act, Digital Markets Act, Data Governance Act, Data Act and General Data Protection Regulation.

- In its draft report Virtual worlds: opportunities, risks and policy implications for the Single Market, the European Parliament "Welcomes the Commission's commitment to monitor the development of virtual worlds; invites the Commission to draft a report on this subject every two years and to transmit it to Parliament and the Council; asks the Commission to pay attention to the potential emergence of problems in the Web 4.0 that already exist in the Web 3.0, such as the proliferation of fake news, infringement of intellectual property rights, cyberterrorism, sexual abuse of minors and cyberbullying, among others"

Q.18. Whether there is a need to establish experimental campuses where startups, innovators, and researchers can collaborate and develop or demonstrate technological capabilities, innovative use cases, and operational models for Metaverse? How can the present CoEs be 162 strengthened for this purpose? Justify your response with rationale and suitable best practices, if any. [4.68]

Nokia Response:

- Metaverse-oriented Centers of Excellence can indeed enable collaboration between all stakeholders and propel development and adoption of Metaverse services. To define the modalities of Metaverse-oriented Centers of Excellence, it can be considered to create a Metaverse community/association with representatives from industry, academia, public sector, citizen organizations for a structured dialogue with policy makers, to identify the needs of the Metaverse sector for collaboration and tune the Centers of Excellence accordingly.

Examples of international best practices

- In Europe, The Virtual and Augmented Reality Industrial Coalition is a platform for structured dialogue between the European VR/AR ecosystem and policymakers. It has produced policy recommendations and a roadmap for sector collaboration and support.

Q.19. How can India play a leading role in metaverse standardization work being done by ITU? What mechanism should be evolved in India for making effective and significant contribution in Metaverse standardisation? Kindly provide elaborate justifications in support of your response. [4.71]

Nokia Response:

The ITU Focus Group on Metaverse has only recently started its activities and is in an exploratory phase, identifying challenges and requirements. This leaves still ample room for active participation in the forum, propose working items and take ownership of them.

A Metaverse community/association with representatives from all stakeholders as referred to in A.18 can identify the most valuable areas for standardization initiatives, e.g. interoperability or user protections.

Centers of Excellence with Metaverse skill sets can generate standardization proposals and bring them to the ITU Metaverse Focus Group.

Q.20. (i) What should be the appropriate governance mechanism for the metaverse for balancing innovation, competition, diversity, and public interest? Kindly give your response with reasons along with global best practices. (ii) Whether there is a need of a national level mechanism to coordinate development of Metaverse standards and guidelines? Kindly give your response with reasons along with global best practices. [4.74]

Q.21. Whether there is a need to establish a regulatory framework for content moderation in the metaverse, given the diversity of cultural norms and values, as well as the potential for harmful or illegal content such as hate speech, misinformation, cyberbullying, and child exploitation?

Nokia Response:

In line with the A.17 to Q.17,

- Existing content moderation regulation for current online services can provide the basis to apply content moderation in emerging Metaverse services.
- A close monitoring of Metaverse experiences and issues can identify additional needs for regulation.
- Align as much as possible novel Metaverse-specific content moderation policies on a global scale.

Example of international best practice

- Europe’s Better Internet for Kids strategy will develop additional resources related to Metaverse service.

Q.22. If answer to Q.21 is yes, please elaborate on the following: i. What are the current policies and practices for content moderation on Metaverse platforms? ii. What are the main challenges and gaps in content moderation in the Metaverse? 163 iii. What are the best practices and examples of effective content moderation in the Metaverse or other similar spaces? iv. What are the key principles and values that should guide content moderation in the Metaverse? v. How can stakeholders collaborate and coordinate on content moderation in the Metaverse? [4.77]

Q.23. Please suggest the modifications required in the existing legal framework with regard to: i. Establishing mechanisms for identifying and registering IPRs in the metaverse. ii. Creating a harmonized and balanced approach for protecting and enforcing IPRs in the metaverse, taking into account the interests of both creators and users of virtual goods and services. iii. Ensuring interoperability and compatibility of IPRs across different virtual environments. Kindly give your response with reasons along with global best practices. [4.80]

Nokia Response:

The existing legal frameworks for IPR for digital content provide a sound basis for IPR policies in the Metaverse. Close monitoring of Metaverse developments is recommended to identify additional regulation needs, and align new policies at a global scale.

Blockchain technology with NFTs can provide a tamper-free, transparent and global mechanism to register creator rights of original digital content and ownership of legal instances of original content. It does by itself however not offer any enforcement mechanisms for intellectual property rights.

It can be expected that the biggest challenge for IPR in Metaverse environments will not necessarily stem from the novel immersive 3D modality, but rather from the application of Generative AI technology in content creation, e.g. to imitate and repurpose protected content. This challenge is not specific to Metaverse environments and manifests itself already today in established online services. Adequate regulation adjustments may be required, preferably aligned on a global scale.

Metaverse interoperability is the main goal of the Metaverse Standards Forum, and its recommendations can serve as global guidelines for standardization and regulation.

Q.24. Please comment on any other related issue in promotion of the development, deployment and adoption of 5G use cases, 5G enabled IoT use cases and Metaverse use cases in India. Please support your answer with suitable examples and best practices in India and abroad

---