AI General Assembly, 1st Session, 2020

Indian Conference on Artificial Intelligence and Law, 2020

Report No. 0110-AIGA-S1-2020-01-REP

Passed by the Assembly with Absolute Majority of 11-0 on October 1, 2020.

Authored by:

Dev S. Tejnani, Sanad Arora, Emmanuel Goffi, Mridutpal Bhattacharyya, Samar Singh Rajput, Anurati Bukanam, Prantik Mukherjee, Prakhar Prakash, Kashvi Shetty;

Executive Summary

Submitted by:
Mr Sanjay Notani, President, AI General Assembly, 1st Session; Abhivardhan, President of the Indian Conference on AI and Law, 2020 and Kshitij Naik, Nodal Advisor, ISAIL.

The Executive Board in the Report for the Day 1 recommends the following considering the quality, purpose and relevance of the scheme of discussion in the Assembly:

- Rights of consumers must be respected and tackled accordingly in the wake of splinternet and its abrasive manoeuvres;
- Governmental participation and collaborative governance can be utilized to assess the development of splinternet in India;
- The principles of Data Erasure, Data Quality and others as emanated from the GDPR, on a ideation perspective can be sought and transformed one-by-one accordingly;
- The issue of cyber security around 5G and ways and means to secure privacy and dealing with disruptive technologies such as the Internet of Things and others have an important significance in the same.
- Corporate responsibility has an intra-perspective in the geopolitics of splinternet;
- Individual responsibilities in using these technologies, based on educational training beyond awareness, based on indigenous and global needs, must be calibrated and decided accordingly. The disruptive and amorphous transformation of splinternet will be strategic and thought leadership based on the nature of sciences will have great significance;

Introduction

- It is imperative to understand that the previous mobile generation networks have solely focused on providing a high-speed voice and data service. However, 5G on the other hand can be deemed to be regarded as something phenomenal. It is not just a network but it is an entire system consisting of high-speed, low latency, and low-power 5G applications, such as the Internet of Things, innovative advancements in the field of machine learning. It can be said that 5G will enable individuals to rapidly develop the infrastructure in their countries and technology could become a part of each country's critical national infrastructure, as well as it can be deemed to be regarded as a core capability on which every other critical national infrastructure sector will depend on. It is said that 5G is capable of offering up to 600x times faster internet speed as compared to the current 4G networks. 5G is said to process data up to 2.7 times faster as compared to the 4G networks and the 5G technology is designed in a

way which would enable users to send data to and from as many as a million devices per square kilometre, compared to the 100,000 devices per square kilometre through which data could be transmitted via 4G networks. 5G is not just limited to being a high-speed network, an important part of 5G specifications are Ultra Reliable and Low Latency Communications (ULLRC) and Massive Machine Type Communications (MMTC). ULLRC allows 5G to enable instantaneous data transfer between two devices and MMTC would allow a large number of users to be connected to a 5G network simultaneously, this can allow for multiple devices to communicate amongst each other with limited to no latency, this can usher an era of autonomous robots all functioning in harmony. For example, 5G is implemented on a mass scale, cars with autonomous driving systems can communicate with each other, essentially eliminating the possibility of road accidents ever happening.

- 5G can exponentially benefit the use of Internet of Things devices (IOT), by helping in transitioning from cloud computing to edge computing. When it comes to cloud computing, the data from an IOT is directly collected and sent to the cloud. Because IOT devices collect huge amounts of data every second, it has become difficult for companies to process and take care of so much data on the cloud. So instead companies have been adopting the technology of edge computing where the data so collected on the IOT device instead of being sent on the cloud will be processed inside the device itself. But this data so collected can be assessed by the companies who make the IOT device which poses a major risk to the privacy of users. Since such IOT devices are connected to a 5G, it can also be prone to hacking. Which is why, privacy can be deemed to be regarded as a major concern and a counter-espionage concern, more importantly, risks pertaining to 5G networks can be deemed to be regarded as cyber-kinetic in nature.

- The consequences of 5G being sabotaged, or being used to overpower the critical build up related to it, can be understood as something which is comparatively more serious that the privacy concerns which are apparent on the face of it and thereby impacting the physical well-being and lives of the citizens or the environment as a whole. The power to transfer or transmit more data, achieve better network responsiveness with the help of lower network latency, thereby reducing energy consumption, which can be rendered possible with the advent of 5G can foster the development of machine-to-machine transformation and communication over 5G. This method of communication can be deemed to be regarded as an essential for various military-related endeavours which the governments of various countries may enable. It is imperative to note here that sensors can be used from a number of locations and these sensors which are on a 5G network can allow the military to generate an unified picture of the battlefield and analyse the surroundings before going ahead with their tactics. This can be deployed with an encrypted communication method and it can provide visibility, command and control. 5G growth can unable the development of AI support whenever the government aims on taking up a mission, it can enable the government to have a clear visual with a motion-to-photon latency with the help of a 5G enabled access to the abundance of computation, which could enable virtual reality, mixed reality and augmented reality and this can be deemed to be regarded as a step towards making the soldiers of the military much more efficient.

- Now, it is imperative to understand that 5G can have a significant impact on how a civilisation works or functions and the decisions pertaining to 5G cannot be made solely on the basis on how profitable it could be for the businesses developing it, however, it is imperative to understand that 5G has certain political consequences also. If one considers India, the framework in India pertaining to Internet governance can be deemed to be regarded as something which is based on the old cliches of Indian Diplomacy. It is imperative for the Indian Judiciary to step out of their lethargy and establish a

comprehensive or a robust piece of legislation pertaining to the sustainable use of 5G and how the Internet of Things is going to pan out.

- India has previously declined the request made at the UN with regards to the direct broadcast of satellite technology in the 1970 on grounds that it would violate its territorial sovereignty, however, the IT sector in India is at present booming and the need to govern the internet is crucial. Internet governance has never been a part of India's plans, however, there exists a dire need for India to work upon a robust regime with regards to Internet governance, if it aims on establishing a 5G network in India. Data localization can be deemed to be regarded as an aspect which needs to be considered primarily. India needs to consider its position on internet governance and how the data localization regime needs to work. It is imperative to understand what is meant by data localisation. Data localization simply means that whichever company in India stores information pertaining to its users, should be capable enough to store and process this data within the Indian borders and the data of its users should be protected. Data localization would enable the data to be stored safely within the territorial limits of a country rather than entrusting the personal data of its citizens to a foreign entity which has its own setbacks or repercussions in the global field. New models of cyber governance laws need to be developed and these models need to be substituted with the existing global stakeholder community.

- Moving on, Cyber-statecraft is something which can be deemed to be regarded as customary, however, the act pertaining to the balkanization of the internet will eventually lead to war and not render peace. The entire aspect revolving around cyber-balkanisation can be divided into two major schools of thoughts, namely security driven and business driven. The security driven aspect school basically enumerates upon national security which is something who's base relies upon the Post-Snowden era. Business driven school of thought on the other hand is a class of section which is an old school that supports splinternet. It is imperative to understand that balkanisation of the internet has innumerable security implications and in particular, innumerable concerns have emerged with regards to surveillance, privacy and how forthcoming attacks with regards to critical information infrastructure operate.

Recommendations and their Basis

1. **Agenda 1: The Scope of Splinternet & 5G Governance in Multilateral Governance & Data Sovereignty Policy**
   a. **1.1: 5G Governance and the Emergence of Splinternet**
      - 5G is difficult to govern at the global level due to the balkanization of the Internet;
      - Nonetheless there are global concerns regarding human rights that need to be tackled at the global level;
      - We have to take into account cultural differences to avoid imposing one perspective over others, namely the Western one;
      - Splinternet is inevitable and norms and regulations have to be in place to promote a democratic form of governance;
      - The need of the hour is a system of transparent monitoring to tackle issues on online freedom and restriction;
      - Understanding the restriction that developing countries face in regard to lack of resources must give way to careful diplomacy where, developing nations have a say in the final establishment;
      - It is important to keep in mind that the main essence of the internet was the absence of boundaries, which is a driving factor for economic growth and development;
      - Applicability and adaptability of any regulative structure is going to be important for a concrete action plan in years to come. And in avoidance of failure of the same;
      - Separate body for legislative, judicial, investigative actions must exist to govern actions of the countries;
      - It is humbly submitted that we have to look at different jurisdictions for formation of EU GDPR debates and the intention behind formation of those policies. Not only EU nations but multi nation jurisdiction;
      - Understand the perspective of the formation of policies and the main agenda behind it.
      - Indian perspective vis a vis perspective of developed nations on formation of those policies help us in understanding the true nature of the policy;
      - Furtherance of awareness spreading to ensure proper understanding of the concepts of splinternet;
      - Suggestion of amendments & regulations to be inserted into the statues to make sure that justice prevails, irrespective of circumstances;
      - Splinternet is a system that is inevitable in the current generation. It cannot be denied that the global governance of the Internet is an ideal solution. However, in this day and age, such a governance structure seems implausible;
      - The roles of various stakeholders are critical to achieving the free Internet. Hence, adopt a multi-stakeholder approach. Non-governmental Organisations, Civil-Society Organisations, and even individuals must advance and advocate for free internet rights;
      - In India, attempts were made through "Facebook basics" and by Reliance towards splinternet which was vehemently opposed by the policy makers and the people at large;

On the other hand, it has slowly made its way under the government's efforts to regulate the contents of the internet;

- The nations that have taken steps to isolate their national internets from the international internet are far better placed to survive all-out cyberwar then the countries that are pushing for a single global internet;

- Countries differ in morality and in the sense of right and wrong. An example could be the difference of censorship laws in a conservative and a liberal government. Splinternet thus has a scope in promoting national interest and restricting anti-social views e.g. fake news on the internet. However, the counter view could be that it would restrict one's freedom of speech;
- On one hand, in 2016 the United Nation declared "online freedom" to be a fundamental human right that must be protected and on the other hand European Union under GDPR gives the right to be forgotten to address the privacy concerns which makes Google inaccurate and non- representative of what a world wide web actually is;
- The international conventions and agreements ratified by the countries should be strictly enforced and any lapse by a country to uphold its international commitments should be met by heavy penalties;

b. **1.2: Data Protectionism & Splinternet**
- Data protection is already a critical issue to be addressed. Data is the "New oil" for which many countries are fighting;
- Need for a global governance that would support and monitor national/local initiative on the matter;
- A global governance would also offer the possibility for every individual all around the world to benefit from protection;
- Need for more training and information towards grassroot people. This can be monitored by the same global structure. The point is to inform people about the ins and outs of data privacy and their digital identity;
- We need to understand the role of the government informing these policies as well as private players and corporates in the market and their roles over the years in formation of those policies related to data protection;
- Role of non-state actors in providing assistance and expert knowledge would allow for more elaborate efforts.
- Further we have to look at the curve as how those policies have affected those nations for better or worse. all this will give us a proper picture portrait of these policies and what we can do to correct it;
- Legislative recommendations aimed towards improving the regulatory frameworks concerning VPNs, proxies, etc, which might prove to be national threats in terms of diplomatic relations, as well as instrumental to terrorism or other threats;

- Discussion on the provisions present in respect to splinternet in order to ensure that human rights aren't affected or rather, infringed;
- Data Protection through data localisation is important to exercise sovereignty on the data a nation has. RBI recently issued regulation to secure all the financial translation data on the servers placed in India. Aadhar data has a humongous amount of sensitive personal data of Indian citizens;
- A concept of different levels of data protection and localisation could be applicable depending on the type and sensitivity of the data. A global standard could be reached upon and through an *internet freedom and transparency index* the nations can be influenced to provide the required protection to their data;
- A GPS enabled data access can be thought of to grant access to a particular type of data to a resident of a particular location. Thus, restricting the access to sensitive data from global access and attacks;
- An international data encryption standard can be set, which needs to be adhered to by the companies to ensure the data security of their stake holders;
- The growing awareness and importance of data protection laws are essential in the context of Splinternet and 5-G. There will be issues that occur amongst states and even within counties;
- Cross-border data transfers are an inevitable practice, and with nations having jurisdiction of the Internet, such data governance will be problematic. The Indian Personal Data Protection Bill (PDP), 2019, has asked to store a copy of India's data. This provision will help prevent manipulation to a certain extent;
- Adjudication authorities grant the Right to be Forgotten under the PDP Bill 2019 as per their discretion. This provision does not allow individuals to have power over their data and lack transparency in using data mechanisms. Therefore, regulations must maintain the rights of individuals along with economic development;

c. **1.3: Data Protection Infrastructure and their Liability Frameworks**
- Data protection must be tackled at the national levels. Sovereignty is a strong hurdle for global monitoring;
- A debate on the balance between financial interests and values must be set. Clear statement of all stakeholders must be available on the subject. Diplomatic (too often hypocritical) statements are counterproductive and prevent from moving forward to any efficient normative instrument;
- The GDPR is a perfect example of such irrelevant and inefficient tool;
- Any protection and liability framework should be assessed in terms of operationalization and accompanied with a regime of sanctions;
- Ethics codes and declaration of intent are not sufficient;
- Education upon the philosophy behind the infrastructures, to ensure absence of bias;

- 5-G will tap into a large market, and governments in the future will rely a lot on such networks. So, if entities controlled by respective states manipulate another state's network, this could lead to the falling of the state's entire critical infrastructure. There is a vast amount of data used by these 5-G network systems;

- Accountability mechanisms and regulations provide specific parameters for entities and developers involved in this 5-G network system, will be an efficient mechanism;

- Huawei is at the helm of recent debate on data protection infrastructure. The ban on it by USA was lifted. The IPR related to 5G is mostly with Ericsson, Nokia, Qualcomm and Huawei only comes at distant 4th position. However, the latter provides the services at a much cheaper rate;

- As Indian telecom industry is under financial stress, it cannot afford a costly solution. Nevertheless, the Indian Govt has formed a 3-year plan for developing indigenous 5G testbeds and Jio recently announced that it has developed the technology on a global standard;

- The Tech is fast changing and the statute is changed by legislature which needs to be expedited replacing them by Tech Savvy policy makers;

Ratified by the Secretariat, Indian Society of Artificial Intelligence and Law.

FINAL