BRAWIJAYA LAW JOURNAL
Journal of Legal Studies
e ISSN 2503-0841
p ISSN 2356-4512
Volume 8 No. 2 October 2021
Nationally Accredited No. 30/E/KPT/2018 Dated 24th October 2018

Need for Revamping Information Technology Laws in India

Ivneet Kaur Walia[1], Dinesh Kumar[2]

[1] Rajiv Gandhi National University of Law, Punjab
Email: ikwalia@gmail.com
[2]Department of Law, Panjab University, Chandigarh
Email: dinesh@pu.ac.in

Submitted: 2021-02-26 | Accepted: 2021-10-05

Abstract: *Homo Sapiens have a distinct characteristic of being superior to other creatures. They owe this superiority not only because they have the power to reason and rationalize but also because they have a tendency to organize themselves as a congregation, which can work in a group at a large scale. The human instinct to improvise on its own inventions, have today resulted in mutation of a world from the stage of abacus to the era of Robotics. For the sake of avoiding chaos and maintaining the sovereignty, every nation strives to eradicate the fear of dominance by the selected elite and hence the need of regulations and the law. The aim of the paper is to highlight the grey areas and limitations existent in Information Technology Laws and focusing on the emerging domains of cyberspace. Its also aims to draw the attention by the policymakers and the legislators to understand the need for amending the Information Technology Act, 2000 for including legal provisions related to emerging issues in cyber space. The analytical research method is used to collect the data based on a systematic review of the existing sources of information and involved qualitative research to analyze the information. The conclusion and suggestions of this paper will definitely be helpful in either drafting or amending a comprehensive law relating to IT keeping in view the evolving technologies and their applications.*

Keywords: cyberspace; data protection; information technology; internet; laws

I. INTRODUCTION

The growth and development of internet is understood in terms of two major phases: *"**firstly**, its development from a military experiment to a civilian utility and **secondly**, in regard to the commercialization of the network"*[1]. In the first scenario, the first phase wandered around the doctrine of 'mutual assured destruction' which regulated the standoff between United States and Soviet Union. During this time an urgent need to develop a communication system capable of surviving a thermonuclear attack was felt. This gave birth to the concept of packet switching, followed by the establishment of Advanced Research Project

[1] John Naughton, 2016, The Evolution of The Internet: from Military Experiment to General Purpose Technology, Journal of Cyber Policy, Vol.1, No. 1, p.7

Agency (ARPA) within the Department of Defense which advanced research in military applications. To encourage the shared resources research amongst the ARPA funded researchers across the United States, Advanced Research Projects Agency Network (ARPANET) was set up. By 1981, Pentagon announced that all ARPANET will be required to adopt TCP/IP, which marks the beginning of the Internet that we use today. During the same time a decision was taken to separate the civilian and military domains of ARPANET which bought about a major transition. In the second phase, after 1995, ushered the era of commercial Internet, the launch of mosaic (the first display graphics inline), was a leap in development of internet and web and triggered the demand for internet amongst general public. Companies like Netscape introduced products like Browser, Netscape Navigator etc. then the growth of these networks has been ever encompassing with https, cookies, audio-video file sharing and its sudden concerns about intellectual property violations, data protections and cyber-crimes, thus calling for the regulatory framework of this spontaneous changing technology.

The world is slowly transitioning from a paper usage mode to the paperless. The Internet and the concept of World Wide Web is drastically mutating the world we are living in. Poverty, famine and wars are no more of greater concern today, when compared to a cyber-attack on a defence establishment or an economic infrastructure of a nation. The usage of internet and a computer system has never acquired a dominant position to an extent as it has done during the COVID-19 times. The complete administration, academics and governance is now communicating using the electronic and digital language. We are no more living in the world of English and French, we now belong to the world of coding, which is now an essential subject for the students in terms of the new education policy in India. The world is spinning at such a velocity that we are unsure of our societal matrix and its ways of functioning with the algorithms. This pandemic somehow marks the beginning of an advanced stage of digital India in making. Years after adapting to the changing dimensions of cyberspace, we still fear of losing our personal and sensitive data and information to an accounted giant.

When too much of matter wanders in the space, that is to say, when too much of information floats in the networks of the cyberspace, there arises a necessity to regulate it. The regulation is to maintain the chaotic bits and bytes into a systematic order to avoid chaos and hence falls the need of enacting laws and strengthening the enforceability regime. There is a necessity to enact or strengthen the Information Technology laws in the country as they form the backbone of social, cultural and economic neurons of the country's biological form. The requirement of having a strong Information Technology legal framework is also essential because the laws of the physical world cannot be applied to the violations and transgressions of the cyberspace. Internet demands both supportive and enabling legal infrastructure.

II. LEGAL MATERIALS AND METHODS

Evaluating the necessity of regulating the virtual space because of its vulnerabilities and societal dependency, the *Information Technology Act*, 2000 was thus enacted by the legislature on the lines of UNCITRAL

Model.[2] The UNCITRAL model emphasized on providing legal recognition to electronic documents and online transactions. It also amended, the other statutes to bring them into conformity with the electronic medium and jurisdiction, for instance, the *Indian Penal Code*, 1860, the *Indian Evidence Act,* 1872, *The Banker's Book Evidence Act,* 1891, *The Indian Contract Act*, 1872 and *The Reserve Bank of India Act*, 1934 etc. Therefore, basically it was an effort to provide legal recognition to all the electronic records. The Amendment in 2008 which was made to the *Information Technology Act*, 2000 further emphasized and made an effort to focus on Information Security. The present law on *Information Technology Act* is self-elaborative about the lack of upgradation or dynamic approach required for digital rule making in India. Though, the *Information Technology Act*, 2000 is the only regimented law in India dealing with digitalization, yet it has been substantially amended just once in 2008. We did notice minor modifications and moderations in certain laws from time to time, but they were all done to cope with some short-term contingencies affecting the political sphere. For instance, the last amendment to the *Information Technology Act*, was made by *Finance Bill*, 2017 which merged and blended the Cyber Appellate Tribunal with Telecom Disputes Settlement and Appellate Tribunal. This modification was again done due to lack of proper grievance redressal body.

One does not need to undertake a serious research on analyzing the grey areas of this law, a cursory look is enough to deduce the limitations, shortcomings and flaws of the existing Information Technology Laws in India. Through this paper, we attempt to make a humble effort in highlighting the areas of the Information Technology laws which require the immediate attention of the legislature, because of the intensity of risk involved for numerous stake holders.

At some places, one would visualize the need to update the already existing provision, at the other, one would see the incompleteness of the statute, where it fails to cope up with the emerging issues in cyber space and from complete different dimension one may wish for an enactment of a complete new law on the subject, because of the magnanimity of the concerns.

The authors have resorted to the use of qualitative analysis. Informal interviews were part of the data collection techniques. The informal interviews and open-ended questions provided flexibility in some aspects of the study. Interactions with members of the legal fraternity gave a clear picture about the practical problems and possible solutions for better implementation and enforcement. The qualitative analysis also involved participant observations for data collection depending upon its systematic planning, validity and reliability.

The authors have also analyzed the legal jurisprudence and drafts of other jurisdictions pertaining to laws and regulations concerning information technology and cyber space to understand the concepts and models that can be well adopted. The paper utilized data located in the primary sources like UNCITRAL Model Law, Budapest Convention, Information Technology Act etc. The Secondary sources in the form of published and unpublished

[2] Bajaj, Kamlesh K, Debjani Nag, 2005, *E-commerce: The Cutting Edge of Business*, Tata McGraw Hill Pub., 2nd Ed, p. 301-304; see also N.S. Nappinai, 2010, *Cyber Crime Law in India : Has Law Kept Pace with Emerging Trends? An Empirical Study*, Journal of International Commercial Law and Technology, Vol. 5, No. 1, p.22-23

reports for example crime records, reports of international organizations were also referred to. The authors have also examined the working papers, articles and surveys dealing with varied component s of virtual space and also referred to international online databases for elaborative understanding of the concept.

III. RESULT AND DISCUSSION

Lack of definition of Cyber Crime or Information Technology Offences

The basic or the foremost error in the statute lies in the fact, that the very term "Cyber Crime" or "Information Technology Offences" is neither defined in the *Information Technology Act*, 2000 nor in its amended version of 2008. This shows the deficiency or lack of certainty on the part of the legislators who couldn't conform to any globally prevalent explanation of the term, nor could determine the relevant factors or components that would define the completion of an offence committed in cyberspace. Thus, one will have to understand the term in a general sense, by assuming that, any offence committed by using a computer system will thus be a Cyber Crime or an Information Technology offence.

Inadequate Legal Framework for Dealing with Cyber Offences

It must be understood that *Information Technology Law*, 2000 and its amended version of 2008 do not form a Cyber Security law in itself. The reason for this is that, even after amending and adding more cyber offences to the list of Information Technology Offences in 2008, the statute still does not cover every kind of Cyber-attack, breach or violation. Moreover, the technology is growing at a faster pace, it's both revolutionizing and reincarnating itself with improvements in technology. Such a constant law will not be able to deal with this scenario whereas, cyber crime is serious issue in India[3]. Resultantly, the cybersecurity system is still germinating and is not fully grown to adapt to the challenges of cyber threats. This is the main reason, why the violations and transgressions in the cyberspace go unreported. The legal framework escapes its obligation of laying down precisely, the duties and responsibilities circumscribing the identities of the stakeholders in the digital and electronic ecosystem. When the laws are inadequate in matter and spirit to protect the citizens of a geographically demarcated area, how can the governmental institutions and organizations be kept safe from such transnational Frankenstein[4].

Jurisdictional Issue

As mentioned above, the transnational character of the crime adds to the basket of the miseries. Although, there are provisions that deal with the jurisdictional concept in the *Information Technology Act*, still they are found to be improper and inadequate and certainly out of question when it comes to implementation and enforceability. There is no clarity about jurisdictional issues when it comes to offences committed in cyberspace. There is ambiguity and uncertainty about the liability of the intermediaries, because of which our policies are still in the germination process. The personnel who are supposedly

[3] Halder, Debarati and H Jaishanker, 2017, *Cyber Crimes Against Women in India*, Sage Publications, vol. xviii, p. 122

[4] Ishveena Singh, 'India's Cybersecurity Laws Inadequate for IoT, Big Data, Cloud and AI' (2020) 30 (August) *Geospatial World* https://www.geospatialworld.net/blogs/iot-big-data-cloud-and-cybersecurity-laws-in-india

required to tackle such issues and concerns, themselves lack the technical knowledge and skills to comprehend upon the problem in hand. They do not have the intricate skills to identify the area or location from where the offence is committed, and to what place is it targeted. They are baffled at the very thought of identifying the place of cause of action or where was the offence completed, as they hardly know the law. In such a pitiable state, how could one assess the security safeguards and procedures required to be installed for raising the bar of cyber security.

Liability of the Intermediary

One must not lose faith in the legislative initiatives of a nation, else the hope would fade away. The recent effort or an example of active rule-making could be seen in the issue pertaining to responsibility and liability of the intermediary or what we call the Internet Service Providers. [5] This initiative was a result of deaths caused due to mob violence, who were incited by messages shared on social media. These incidents prompted the government to lessen the protection given to intermediaries and bringing them to books for not regulating the content posted online. The Inter-Ministerial Committee chaired by Rajiv Gauba, (Home Secretary, in 2018) submitted its report to the Home Minister concerning mob-lynching incidents that happened in the country. They identified the circulation of fake messages on the social media to be the cause of such incitement. The Committee condemned these acts of provocation and incitement caused due to circulation of fake news and rumors and laid down certain recommendations for instance, the Committee recommended the appointment of Superintendent of Police in each district as the nodal officer who would take legal action against the perpetrators of mob violence. The Committee had also taken up the matter and discussed with representatives of the Google, Facebook and Twitter to take all possible measures and eradicate or filter the objectionable content. Furthermore, the Committee is also formulating guidelines that would initiate the grievance redressal over a complaint in few hours. The new intermediary guidelines namely *Information Technology [Intermediaries Guidelines (Amendment) Rules],* 2018 so formulated in the light of Section 79 of the *Information Technology Act*, also require the companies to respond to complaints not only on orders by court and government agencies but also on the request of general public. This will cut down the excuse which was taken earlier by these companies, stating that they would need thirty-six hours to address the complaint as most of the companies are based in West Coast of America and there is a time difference. It was also recommended by the Committee that all such companies will place one such grievance officer in India to avoid such delays. The rules of 2018 as mentioned above imposes an obligation on the intermediaries to prohibit publication of certain type of content by including a provision in their terms of agreement. The draft rules prohibit a new category of information which threatens 'public health or safety'. This further raises issue of violation of freedom of speech and expression but that is more of a duty on judiciary to tackle the issue in its own way. The formulation of such guidelines along with the attentiveness and sensitivity of the government on this matter is a welcome step, but we could benefit from

[5] see also, Bainbridge, David, *Introduction to Information Technology Law* (Trans-Atlantic Publications, 2007), p.24

this only if we know the law and safeguard it.[6]

Implementing the Struck Down Section of Information Technology Act, 2000

The officials of the police department are still registering cases and detaining persons under the already struck down provision of Section 66A of the *Information Technology Act*, 2000.[7] This Section has already been struck down by the Hon'ble Supreme Court of India in 2015 in the case of *Shreya Singhal* v. *Union of India*[8]. A recent case was noted in the year 2018 in Guntur region of Andhra Pradesh, where a man was arrested on the charge of impersonating as a woman on a dating app named Locanto, and asking for money. This man cheated nearly 507 people of Rs 21.58 lakh. Now while police booked Reddy (accused) under Section 420 (Cheating) of the *Indian Penal Code*, 1860. The police also registered a case under Section 66A of the *Information Technology Act*, 2000 on the ground of misleading people through electronic communication. Many of the police officers are not aware of the judgment and continue to abuse and misuse the power given under this Section. The police officials excuse themselves of this responsibility on the pretext of not being aware of the Supreme Court judgments on the ground that such information is not circulated to them or to their departments from higher offices. Therefore, such incidents have become a general routine affair, where the enforcement agencies easily ignore the Supreme Court rulings or even the amendments made by legislature on the pretext of ignorance of law[9].

Lack of Updated Procedural Law and Human Resources

The law relating to the Information Technology in India relies completely on *Code of Criminal Procedure,* 1973 for investigative, evidentiary and enforceability mechanism, but by doing this we face with certain technical limitations. For instance, the *Code of Criminal Procedure*, 1973 in India drafted with the intent of dealing with acts or omissions happening in the real spatial world. It is inadequate in its very molecular substance when question comes to dealing with matters concerning virtual or cyber matrix. Moreover, the police personnel are not well acquainted and equipped with information and growing technological infrastructure. Lack of technical knowledge and skills on this subject will lower the benchmark of the investigation process and will leave the probe addressed inadequately. In reference to these issues, certain States have set up Cyber Cells with Cyber Forensic labs and are also becoming resourcefully adequate in terms of staff and technology. The government is also pondering upon the thought of amending the existing the Information Technology law, so as to appoint a nodal investigative officer of atleast the rank of a Deputy Superintendent of Police (DSP). Yet, it becomes difficult to

6 Meghna Bal, 'India's Information Technology Act Is Set to be Changed – What Should be Reworked?' (2020) 30 (August) *The Wire* https://thewire.in/law/india-information-technology-act-changes/amp/

7 Pallavi Kapila, 2020, *Cyber Crimes and Cyber Laws in India: An Overview, in book: Contemporary Issues and Challenges in the Society,* New Era International Imprint, p. 9-10

8 *Shreya Singhal* v. *Union of India* (2013) 12 SC 73.

9 Gopal Sathe, 'The Supreme Court Struck Down Section 66A of the IT Act in 2015, Why Are Cops Still Using It to Make Arrests?' (2020) 3 (August 30) *Huffpost* https://www.huffingtonpost.in/2018/10/15/the-supreme-court-struck-down-section-66a-of-the-it-act-in-2015-why-are-cops-still-using-it-to-make-arrests_a_23561703/? guccounter=1

comprehend, as how placing a higher rank policer officer to investigate a cybercrime issue would fill in the gaps of such deficiencies. No literature highlights the lack of procedural laws and infrastructure when it comes to cyber space.

Need for Setting up Cyber Cell Units and one Autonomous Body to Check Policy and Practice

To support stringent policing, we need to set up Cyber cells at district level and their enforcing regimes at the State level. A Coordination Centre for Cyberspace may also be set up at a national level to facilitate data storage, data sharing, easy access to information etc. Establishment of such facilities at these levels will ensure coordination amongst various functionaries and departments. It would also enhance knowledge sharing which will further endorse upgrading of the infrastructure uniformly and such an establishment may also encourage research and development in the field of Information and Communication Technology. Many of the States have already initiated the process of setting up such departments at district level. But to have a uniform structure, certain guidelines may be followed. The important points that are required to be kept in mind while establishing such infrastructure includes, *firstly*, a Charter, which would lay down not only the roles, responsibilities or the duties of the personnel but also the procedure, which one would follow on receipt of the complaint. *Secondly*, Human Resources, which underlines the requirement of recruiting a specialized staff, which is not only technically sound and skillful, but also well aware of the technological advancements around him. The staff may not exclusively be constituent of people from police department but may also include experts equipped with computer handling techniques. *Thirdly*, Supervision, the infrastructure and human resources at different levels can interact freely and without any biases or influences only if a supervisory role is assigned to the establishment at the national level. This supervision is necessary or rather essential because these cells will have to cooperate and coordinate with government agencies and the evidence given by them or a report on evidence provided by them, may be of much evidentiary value. Hence, supervision is important to maintain the authenticity, credibility and integrity for the functioning of these cells.

Surveillance Reform

On scrutinizing the prevalent laws and policies one may easily infer that India is not a surveillance country. There is also an absence of substantial base to regulate surveillance in the country and one can substantiate this argument by looking at the Pegasus spyware controversy. There is no data protection law in the country as compared to GDPR or similar regulations. All the provisions regarding data protection are scattered in different rules and regulations but its implications are not discussed anywhere because there is a lack of legislation. One may come across scattered provisions on surveillance in statutes such as, the *Telegraph Act*, 1885 and Section 69(1) of the *Information Technology Act*, 2000. The problem with *Telegraph Act* is that it is an archaic legislation and is certainly not in conformity with technological revolution and issue with Section 69(1) is *firstly*, that it is not adequate, and *secondly*, it limits the scope of surveillance as it allows counted few to decrypt. The matter pertaining to having stricter provisions, or rather a legislation came into scene after the controversy triggered in 2019, when a spyware named

Pegasus alarmed privacy concerns across the world. India too was affected by this spyware. This spyware hacks the information of the citizens of a nation. The spyware is created by a group called NSO (Niv, Shalev and Omri) which surprisingly deals with only government's and their agencies. This indicates that induction of such a spyware can only happen with the knowledge and consent of the Government, which as a consequence raises eyebrows at the administration. It is also pertinent to mention that the government did not order any investigation or probe into this matter.[10]

Considering such careless approach of the government, the Internet Freedom Foundation (NGO), emphasized upon the necessity of such surveillance reforms, which would protect citizens against the use of malignant malware and spyware, by way of offering privacy 'protection by design'. The Government notification allowed ten national agencies to decrypt the information and have the surveillance rights. This is certainly prone to abuse and privacy violations. The Inter-Ministerial Committee that was set up for examining role of Intermediaries also made a mention about the rights of surveillance. It was in the exercise of power given under Section 69(1) of the *Information Technology Act*, 2000 and Rule 4 of the *Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules*, 2009 that the competent authority got the power to authorize the Security and Intelligence Agencies for the purposes of interception, monitoring and decryption of any information which is generated, transmitted, received or stored in any computer resource under the said Act. These rules have circumvented the more specific rules that were laid down for phone tapping or digital communication as provided by the *Telegraph Act*, 1885 and have lent more scope and space to these agencies, which may arbitrarily violate privacy norms and raise concerns.

Information Technology (Amendment) Bill, 2018

India is yet to pass the *Information Technology (Amendment) Bill*, 2018. The reasons for the delay are unexplained as this amendment bill was introduced in the parliament when the world was suffering from an online catastrophe by the name of 'Blue Whale Challenge'. This online game caused serious psychological damage and induced individuals to end their life. This is just one example of many other online games that induce infliction of self harm. The bill intended to insert certain provisions in the existing Information Technology laws that would prohibit publishing or transmission of any material repugnant to the cultural ethos (sought to introduce Section 67BA) and also make hosting of dangerous online games as a punishable offence (sought to introduce Section 79B). The delay in passing of the Bill and non-insertion of these provisions is only making the nation more vulnerable, causing seismic waves in the socio-cultural fabric of our society.

The Indian Institute of Information Technology Laws (Amendment) Bill, 2020

Another Bill in the pipe line which is pending in the parliament is the *the Indian Institute of Information Technology Laws (Amendment) Bill*, 2020. This bill intends to amend the *Indian Institutes of Information Technology (Public-Private Partnership)*

[10] Anam Ajmal, 'Need Surveillance Reform, Privacy Law: Cyber Experts' *The Times of India*, 2020 30 (August) https://timesofindia.indiatimes.com/india/need-surveillance-reform-privacy-law-cyberexperts/articleshow/7186 0462.cms

Act, 2017. The Act declares certain institutions as institutes of national importance. The amendments will ensure more research in the field of Information Technology and will help us build up a cyber community and workforce that can work in this industry. The Bill when passed can bridge various gaps in reference to upgrading of technological infrastructure and human resources.[11]

Data Protection and Privacy

The word that's trending more than the data packets on a network in the cyber space is the term 'Big Data'. Big data analytics is the most upcoming advancement of technological era. The responsibility of analyzing and storing data is a big responsibility as it jeopardizes privacy. Accountability, Accessibility and Security principles require a privacy law to have an important component like supervisory assignments and redressal mechanism. In the present times, India neither have any such strong regulatory authority nor any privacy or data commissioner. Moreover, deficiency has also been felt in finding the independent data of specific cybercrime, which is difficult to ascertain, though National Crime Record Bureau provides an overall data for cybercrimes. Certain data's also need to be generated for instance, data related to national expenditure on cybersecurity, data pertaining to businesses that have suffered from crimes like phishing or data breaches pertaining to thefts of finances or information from governmental institutions.

The increased activities of the individuals in the cyber world has initiated an 'information sharing culture'. The laws dealing with Data Protection in India presently includes, **firstly,** the *Personal Data Protection Bill*, 2019 which is currently pending in the parliament. **Secondly**, Section 43A of the *Information Technology Act*, 2000 (amended in 2008), which deals with security practices and procedures relating to possessing, dealing or handling of any Sensitive Personal Data or Information (SPDI) [12] . **Thirdly,** the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules*, 2011, but the rules do not exclusively deal with the right to privacy.

The *Personal Data Protection Bill*, 2019 which is still pending in the parliament is the online exclusive legislative piece of work which will "ensures protection to privacy of the individual[13] as a fundamental rights and privacy protection as a vital part of information privacy" [14] . When the Bill becomes an Act, it will supersede Section 43-A of the *Information Technology Act*, 2000 (amended in 2008) and the *Sensitive Personal Data or Information Rules*, 2011.

Other regulators, which provide for guidelines in regard to data privacy and data protection in India include the Reserve Bank of India which mandates all system providers to store the payments data in India, certain cyber security guidelines have also been

[11] Devika, 'The Indian Institute of Information Technology Laws (Amendment) Bill, 2020,' (2020) 30 (August) *SCCONLINE* https://www.scconline.com/blog/post/2020/03/06/the-indian-institutes-of-information-technology-laws-amendment-bill-2020-introduced-in-lok-sabha/

[12] see also, Deva Prasad M and Suchitra Menon C, 2020, The Personal Data Protection Bill, 2018: India's Regulatory Journey Towards A Comprehensive Data Protection Law, International Journal of Law and Information Technology, p.2

[13] Aditi Subramaniam and Sanuj Das, 2021, The Privacy, Data Protection and Cybersecurity Law Review: India, The Law Reviews, Ed. 8, p.1

[14] Mandeep Kumar and Puja Kumari, 2020, *Data Protection & Rights to Privacy: Legislative Framework in India*, Journal of Critical Review, Vol. 7, No. 11, p. 3427

issued for insurance companies in 2017 by the Insurance Regulatory and Development Authority of India. Moreover, Security Exchange Board of India (SEBI) has also in 2016 provided Cyber Security and Cyber Resilience Framework of Stock Exchanges, Clearing Corporations and Depositories. Furthermore, Ministry of Health and Family Welfare notified the draft on Digital Information Security in Healthcare Act and invited for Public Comments.

In addition to this, a concept of 'Internet of things' is evolving as a system or a web which interconnects individuals, things and the information technology systems reactive to physical and virtual forms of information. It aims to enhance and improvise the communication between individuals, systems and things etc. If such an interaction takes place amongst them, it will obviously result in personal information sharing and voluminous data exchange resulting into privacy and data protection issues. In the light of this government has released a draft on 'Internet of Things Policy' in 2015. These concepts are giving rise to 'Machine to Machine' ecosystem and introducing concepts like Machine learning. Every such development breeds on already existing information and data floating in the cyberspace. Thus, safeguarding the privacy and data of citizens attain priority concern in this field.[15]

Artificial Intelligence

When the computers acquire or imitate human intelligence, where they are able to foresee or visualize the requirement and also perform speech recognition, that marks the entry point to the world of Artificial Intelligence. Indian law neither has any provision nor any law to deal with ethical, legal and regulatory implications of Artificial intelligence. In the other parts of the world where the explosion of Space X Falcon 9 is being questioned and accidents of the driverless car of Tesla's are being regulated by the laws of the western world. India is still struggling to bring the aggregators such as Uber and Ola to books when legal issues or conflicts arises. In India, we neither have the literature on product liability nor have we built jurisprudence on tort of wrongful death. For every such wrong, we invoke Section 43A of the *Information Technology Act*, 2000 (amended in 2008) and proceed in Consumer courts for a legal action either for defect in product or because of deficiency in services.

Though, the Ministry of Electronics and Information Technology has released four Artificial Intelligence Committee Reports in 2019 which deals with Platforms and data on Artificial Intelligence, using Artificial Intelligence in national missions and programs in key sectors, analyzing and mapping technological capacity of imbibing Artificial intelligence technology and lastly the cybersecurity issues, still a long path needs to be treaded to come at par with the other countries of the world. In 2018-2019 budget NITI Aayog is mandated to establish the National program on Artificial Intelligence. Though, it's a positive step and a commendable one too but on the other side it also reflects our unpreparedness and tenderfoot on this issue.

Another issue pertaining to Artificial Intelligence is that Indian law does not recognize Artificial Intelligence entity as a legal person. This raise concerns under various laws, for instance, the Indian Contract Law mandates both the parties

[15] Vrinda Bhandari and Renuka Sane, 'Analysing the Information Technology Act (2000) from the Viewpoint of Protection of Privacy' (2020) 30 (August)*The Leap Blog* https://blog.theleapjournal.org/2016/03/analysing-information-technology-act.html?m=1

forming a contract to be competent legal persons. Thus, Artificial Intelligence entity cannot enter into a valid contract both in the cyber space and in the physical space. There are concerns that in future the human workforce will be replaced by the workforce of the artificially intelligent robots and our labor laws are ill equipped to deal with such a scenario. A conflict will also arise in the field of Intellectual Property law where the creation of the Artificial Intelligent being will be questioned for grant of Intellectual property protection.[16]

Blockchain Technology and Cryptocurrency

Most of the blockchain based projects in India fail to move beyond a point because of the lack of laws and regulatory imperfections.[17] As the provisions of the *Information Technology Act* precludes the usage of digital signatures to transactions or documents involving immovable property. This restricts and limits the usage of blockchain based applications in a country where majority legal issues and conflicts pertain to property. Now, in regard to cryptocurrency, the Supreme Court of India has granted a legal back to Bit Coins but still the country lacks a proper legal framework. In July 2019, Government released draft legislation, '*Banning of Cryptocurrency and Regulation of Official Digital Currency Act*, 2019' which seeks to ban any person from 'mining, generating, holding, selling, dealing in, issuing, transferring, disposing of or using cryptocurrency in the territory of India.

Also, in September 2019, the Ministry of Finance distinguished the categories of crypto currencies, specifically, Utility tokens and Security tokens. Due to lack of legal provisions, the burden falls on the shoulders of the Reserve Bank of India to issue cautionary circulars in this regard.[18]

There is a lack of conceptual jurisprudence in the national context, when it comes to emerging disruptive technologies like blockchain or adaptation of Artificial Intelligence techniques in the industrial sector. Certain sections of the Information Technology Act, 2000 and 2008, needs a careful examination like, Section 69A, 43A, 67C etc. The research is to be done while maintaining a delicate balance between emerging technologies and constitutional rights under Article 19 and 21. When we already have such immense research gaps are we ready for dealing with the drone technology, cryptocurrency, dome systems in military applications or for combating an army of killer robots.

IV. CONCLUSION AND SUGGESTIONS

To conclude, one may say that the list of gaps and limitations is never ending as the sphere of the virtual world is acting like a black hole. The laws enacted or amended today must resonate with necessities of the future world. One cannot make imperfections perfect in an ever-stretching domain, but

[16] Devika, 'Government Releases- Artificial Intelligence Committee Reports' (2020) 30 (August) *SCCONLINE* https://sccblog-linux.azurewebsites .net/post/2019/12/05/government-releases-artificial-intelligence-committees-reports/.

[17] See also NITI Aayog, 2020, Blockchain: The India Strategy (towards enabling ease of business, ease of living, and ease of governance) part 1, Draft Discussion Paper, NITI Aayog , p.28-30

[18] Bhavana Alexander and Kayal Manivannan, 'Disruptive Tech like Blockchain is Here to Stay, Law Will Have to Simply Catch Up' (2020) 30 (August) *The Economic Times* https://economictimes.indiatimes.com/small-biz/security-tech/technology/disruptive-tech-like-blockchain-is-here-to-stay-law-will-have-to-simply-catch-up/articleshow/59397014.cms?utm_ source=content ofinterest&utm_ medium=text & utm_campaign=cppst.

norms can certainly be set up using terms like 'technology collateral or incidental thereto' with every such provision which will indicate any advancement in technology. Smart drafting of the laws in the ever-advancing world of networks and technology will lessen the call for over legislation, re-enactment and unending amendments. The government's role will always remain *a priori* and quintessential in matters of drafting policies, laws and regulations. However, for now, an immediate and urgent attention is required from the side of the government to update the laws, as the whole nation is living and even functioning in the virtual space more than the physical one. The state must enact stringent laws for intermediary liability, digital ethics and immediate redressal of grievances related to cyber space besides urgently working on Data Protection Bill to deal with privacy concerns. It's high time to provide a regulatory regime for emerging technologies like blockchain, cryptocurrencies and drone etc. We have adapted to Artificial Intelligence and Real time intelligence for prevention of cyber intrusions and violations.

Also, no research is complete without adding an element of innovations. For dealing with regulatory grey areas, specific innovations can be put in place for instance: Intuitive Intrusion Detection. This application defends against malicious cyber-attacks, without having to be taught what those threats may look like, Simple Image Preview in Live Environment (SImPLE), an application can be used in streamlining digital forensic investigations. This application enables rapid identification of offensive and illegal digital material etc.

REFERENCES

Books and Reports

Bainbridge, David, *Introduction to Information Technology Law* (Trans-Atlantic Publications, 2007)

Bajaj, Kamlesh K, Debjani Nag, *E-commerce: The Cutting Edge of Business* (Tata McGraw Hill Pub., 2nd Ed., 2005)

Ministry of Electronics and Information Technology, Government of India, *Artificial Intelligence Committee Report*, 2019 (July) http://www.meity.gov.in/artificial-intelligence-committee-reports

Pallavi Kapila, 2020, *Cyber Crimes and Cyber Laws in India: An Overview, in book: Contemporary Issues and Challenges in the Society*, New Era International Imprint

NITI Aayog, 2020, Blockchain: The India Strategy (towards enabling ease of business, ease of living, and ease of governance) part 1, Draft Discussion Paper, NITI Aayog

Journals

Aditi Subramaniam and Sanuj Das, 2021, The Privacy, Data Protection and Cybersecurity Law Review: India, The Law Reviews, Ed. 8

Deva Prasad M and Suchitra Menon C, 2020, The Personal Data Protection Bill, 2018: India's Regulatory Journey Towards A Comprehensive Data Protection Law, International Journal of Law and Information Technology, Vol. 28, No. 1.

Halder, Debarati and H Jaishanker, *Cyber Crimes Against Women in India*, Sage Publications, vol. xviii, 2017

John Naughton, 2016, The Evolution of The Internet: from Military Experiment to

General Purpose Technology, Journal of Cyber Policy, Vol.1, No. 1

Mandeep Kumar and Puja Kumari, 2020, *Data Protection & Rights to Privacy: Legislative Framework in India,* Journal of Critical Review, Vol. 7, No. 11

N.S. Nappinai, 2010, *Cyber Crime Law in India : Has Law Kept Pace with Emerging Trends? An Empirical Study*, Journal of International Commercial Law and Technology, Vol. 5, No. 1.

Internet

Ajmal, Anam, 'Need Surveillance Reform, Privacy Law: Cyber Experts' *The Times of India*, 2020 30 (August) https://timesofindia.indiatimes.com/india/need-surveillance-reform-privacy-law-cyberexperts/articleshow/71860462.cms

Alexander, Bhavana and Kayal Manivannan, 'Disruptive Tech like Blockchain is Here to Stay, Law Will Have to Simply Catch Up' (2020) 30 (August) *The Economic Times* https://economictimes.indiatimes.com/small-biz/security-tech/technology/disruptive-tech-like-blockchain-is-here-to-stay-law-will-have-to-simply-catch-up/articleshow/59397014.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

Bal, Meghna, 'India's Information Technology Act Is Set to be Changed – What Should be Reworked?' (2020) 30 (August) *The Wire* https://thewire.in/law/india-information-technology-act-changes/amp/

Devika, 'The Indian Institute of Information Technology Laws (Amendment) Bill, 20, https://www.scconline.com/blog/post/tag/the-indian-institutes-of-information-technology-laws-amendment-bill-2020/0,' (2020) 30 (August) *SCCONLINE*

Singh, Ishveena, 'India's Cybersecurity Laws Inadequate for IoT, Big Data, Cloud and AI' (2020) 30 (August) *Geospatial World* https://www.geospatialworld.net/blogs/iot-big-data-cloud-and-cybersecurity-laws-in-india

Sathe, Gopal 'The Supreme Court Struck Down Section 66A of the IT Act in 2015, Why Are Cops Still Using It to Make Arrests?' (2020) 3 (August 30) *Huffpost* https://www.huffingtonpost.in/2018/10/15/the-supreme-court-struck-down-section-66a-of-the-it-act-in-2015-why-are-cops-still-using-it-to-make-arrests_a_23561703/? guccounter=1

Vrinda Bhandari and Renuka Sane, 'Analysing the Information Technology Act (2000) from the Viewpoint of Protection of Privacy' (2020) 30 (August)*The Leap Blog* https://blog.theleapjournal.org/2016/03/analysing-information-technology-act.html?m=1

Acts

The Banker's Book Evidence Act, 1891,

The Banning of Cryptocurrency and Regulation of Official Digital Currency Bill, 2019

The Code of Criminal Procedure, 1973

The Finance Bill, 2017

The Indian Contract Act, 1872

The Indian Evidence Act, 1872,

The Indian Penal Code, 1860,

The Information Technology Act, 2000

The Personal Data Protection Bill, 2019

The Reserve Bank of India Act, 1934
the Sensitive Personal Data or Information Rules, 2011
The Telegraph Act, 1885

List of Cases

Shreya Singhal v. *Union of India* (2013) 12 SC 73