International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 3, March-April 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Critical Analysis of Technology Law in India with Reference to Foreign Mechanism

Jyotirmoy Banerjee[1], Pooja Banerjee[2]

[1]Assistant Professor, Faculty of Law, Vivekananda Global University, Jaipur, Rajasthan, India
[2]IT Faculty, Billabong High International School, Malad, Mumbai, Maharashtra, India

ABSTRACT

During the past few decades, we have witness some of the most exponential growth in our field of technology, whether it is a matter of law, social framework, economic or any other manner in which it has intersected various disciplines. Starting from the UN General Assembly Resolution leading to the approval of the Information Technology Act, further leading to the enactment of the Modern Electronic Trade Law. In reference to which we observed that how the right to privacy modified by the growth of information technology, and after which the technology has changed its contents for the protection of their legal interests. In this technologically evolved world, data is the new currency. As India, has no comprehensive data protection legislation and privacy legislation. The existing policies and laws are, in essence, sectoral in nature. These Sectoral Laws pertain to the IT Law, 2000. It is also observed that how the amendment to the Information Technology Act which entered into force in February 2009 with the presidential assent, has made a crucial impact in India in reference to the IT Laws, stated that information confidentiality constitutes as a part of our privacy right and stated that confidentiality included the right to preserve the personal identify.

KEYWORDS: *Privacy, Technology, Data Protection, Information, Supreme Court*

How to cite this paper: Jyotirmoy Banerjee | Pooja Banerjee "Critical Analysis of Technology Law in India with Reference to Foreign Mechanism" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-3, April 2022, pp.46-53, URL: www.ijtsrd.com/papers/ijtsrd49462.pdf

IJTSRD49462

INTRODUCTION

At a moment of transformation, we have a time when a cluster of technical changes takes place under the terms of economic production and human freedom, and are mostly governed by the law. Law already is and will remain a major field in which circumstances for the future are being negotiated, but it cannot be considered unless the technological, economic and social framework in which it functions and the historical moment when it intersects with other disciplines are understood. A systematic understanding as to how technology affects life and how law interacts with technology is a prerequisite for comprehending the stakeholders and ramifications of the current institutional struggles.

The technology "*from the Greek word techne, art, skill, craft and word-logy*" is a collection of tools including machinery, changes, arrangements and procedures employed by people. This collection includes machines and processes. Engineering is a field in which new technologies are studied and designed. The ability of both humans and other animal species to manage and adapt to their natural surroundings is substantially affected by technology. The phrase can be used in general or in particular domains – construction technology, medical technology and information technology are examples.

HISTORY OF TECHNOLOGY LAW

The UN General Assembly Resolution of 30 January 1997 led to the approval of the Information Technology Act leading to the enactment of the Modern Electronic Trade Law on International Trade Law. It was drafted in July 1998 by the Department of Electronics (DoE). Only on 16 December 1999, when a new IT Ministry was established could it be established in the department. But it was affected by certain e-commerce proposals and issues concerning the World Trade Organization (WTO) obligations in the trade industry. Once the draught law had been put

forward in parliament, after requests and suggestions of Members, the bill had been referred to the 42-member Parliamentary Standing Committee. One of the extensively discussed ideas was that an owner of a cybercafe should keep a register to record the identities and addresses of everyone that visited its café and also a list of the sites that were surfing. This was proposed in order to reduce cybercrime and make it easier for a cybercriminal to locate him quickly. At the same time, however, it was mocked since it would overwhelm the privacy of a net surfer and would be unsustainable. In its final draught, the IT Ministry withdrew this idea.

EVOLUTION OF TECHNOLOGY LAW

The networked personal computer inverts the stable reality of over 150 years of the capital structure of information production and interchange. While the exact figure is impossible to identify, between 600 million and one billion individuals worldwide already possess the fundamental physical capital needed to reduce knowledge, information and culture and to take part in the world economy that focuses on it.

So, nearly a milliard individual now has the freedom on the world to choose whether they want to develop knowledge or culture - they are able to do so already with the physical needs and human intuition, wisdom and creativity. You don't require a business plan for writing software to fulfill your needs. They can compose it and find others who work with them to improve it if they know how to do it.

This is the basic reality demonstrated by the extraordinary success of the creation of free and open-source software. Over a million programmers take part in tens of thousands of projects, among which the most important functions for Internet communications are well recognized and certain projects have been taken up in the face of a strong but ultimately failed competition from proprietary companies.

Thirty thousand persons can come together to build a free online encyclopedia such as Wikipedia, a substitute for most existing online encyclopedias but not for the Encyclopedia Britannica yet. Examples are already legionary and we have relatively strong economic models to explain why the generation of common information and peer production in general and why the two production kinds are sustained under circumstances that are characteristic of a networked information environment.

HOW IS TECHNOLOGY LAW HELPING THE SOCIETY?

The legislation in our society is not simply meant to manage our behavior: it is designed to bring social programmes into practice. For instance, some regulations give compensation for employees wounded at work, medical attention and student loans who may not otherwise be able to go to university.

Fairness is another objective of the law. This means that some fundamental personal rights and freedoms, for example freedom and equality, must be recognized and protected by legislation. The Act also ensures that strong groups and people do not take undue advantage of weaker persons through their dominant positions in society.

As with the right to privacy modified by the growth of information technology, the technology has the ability to change its contents of protected legal interests. Telecommunications' so-called technological convergence has removed aspects that have characterized telecoms as a natural monopoly, opened up the market to a possible number of companies, and improved free market competition in the field. The same applies to the disparate distinction between Article 15 and Article 21 of the Constitution of Italy. For example, when freedom and secrecy are at stake, the former is traditionally enforced. Lastly, freedom of expression is protected for the general public.

Law could potentially apply new technologies to achieve objectives that other technologies in the past have pursued: the e-document, e-signature, e-money payments, contract completion, etc. In all these cases, new regulations provide the possibility of using digital technology to achieve this or that goal, achieved in the past by other technologies.

Technological rules are characterized by the qualities of these technologies. One thing, for example, is to have rules on the matter (atoms), another is to have rules on bits. In other circumstances, it implies that conceptions that typically pertain to material things (such as possession and ownership) must be reconstructed or new concepts used (such as the ideas of title and legitimization in the case of dematerialized financial instruments).

In the past, the role of technology in creating new products was true of the new value of creation, which resulted in the emergence of a new copyright after a protracted procedure. This has happened for databases in recent years (of human tissues for example, but several other examples may be offered). The law is always faced with the need to regulate new, previously unknown commodities. The technological development also affects the source and structure of the rules. Legal systems occasionally prefer to govern certain occurrences by using

international instruments or non-external regulatory structures (for example codes of conduct).[1]

ROLE OF DATA IN TECHNOLOGY LAW OF INDIA

The data is something all around us and is basically created in anything we do. We deliberately share the data and generate the data when we accomplish something. Travel, order or transport a meal, for example. The data is unsure when the data is of considerable value and a number of organizations are willing to purchase such a data strategy. In this technologically evolved world, data is the new currency. Notwithstanding all the information known, the data potential is not yet fully known. New forms of technology are being produced and new applications are being developed to increase its value. In this respect, there are various questions: Who is the data of this kind? Who is supposed to approach such information? What limits must such data be on manipulation? Due to these questions, lawyers around the world continue to strive to understand this fundamental notion of law.

Now when things are highly critical, several governments are asking for and seek the data of businesses and citizens. In the meanwhile, are there questions such as about a person's privacy? Can data be requested to support these basic services, travel or government interests? Would domestic security overcome current privacy concerns?

On 24 August 2017, the Court of Last Resort in India concluded that privacy rights were seen as a basic right provided in Part III of the Indian Constitution. A decision as such will be generalized and all legislation and regulations will be established. The new legislation would be tested for criteria equivalent to laws which replicate personal freedom unauthorized and tested in accordance with Article 21 of the Indigenous Constitution. After all, everybody has questions about its limitations and borders concerning the right to confidentiality.

India has no comprehensive data protection legislation and privacy legislation. The existing policies and laws are, in essence, sectoral in nature. These Sectoral Laws pertain to the IT Law, 2000, which lays out laws governing the process of gathering, use of private information, and the sensitive data or date of the corporate body' in India. The Government oversees the wording of detailed law that contributes to the protection and privacy of data. More efforts are needed to help a panel of privacy experts led by Justice A.P. Shah, formerly a High Court of Delhi Judge, which tabled an extensive report on October 16, 2012. Further efforts are necessary in this regard.

The Government then appointed an expert committee led by Justice Sri Krishna, the preceding judge of Last Resort in India, which reviewed the issues concerning data preservation in India as well as specific suggestions that the Central Government should make in the best interests of the principles of data protection in India.

In the middle of 2018, the Commission submitted its report. Independently, a discussion paper on privacy, ownership and data security in the telecommunications industry was proposed by TRAI. The recommendation by our Committee on Budgetary Funding, within RBI, led to a data protection framework based on rights which was contrary to the premise of employing consent as a first Data Protection Mechanism to improve household financial results.

Data is something around us that is almost generated in whatever we do. We deliberately share the data and generate the data when we accomplish something. Travel, order or transport a meal, for example. The data is unsure when the data is of considerable value and a number of organizations are willing to purchase such a data strategy. In this technologically evolved world, data is the new currency. Notwithstanding all the information known, the data potential is not yet fully known. New forms of technology are being produced and new applications are being developed to increase its value. India currently has no comprehensive data protection and privacy legislation. The existing policies and laws are, in essence, sectoral in nature. The sectoral laws are associated with the IT Act, 2000 and so regulations govern the process of collection, the use by a company in India of private information and sensitive data.

The data plays a vital role in the world today and its protection has become an enormous workload, since data breaches and safety are in major jeopardy. Data protection is critical and legislation relating to the protection of the digital information of a person or of an organization as a whole is regularly updated. In India, there are numerous issues of privacy addressed in the case that legislation and new laws are made, as legislation is learned and developed.

Whether or not the "*right to protection*" is a major right, the Supreme Court has initially examined the

[1]Nabarun Chandra Ray, 'Law and Technology', *Lawctopus,* (Dec., 23, 2014) https://www.lawctopus.com/academike/law-and-technology/ accessed 29 August, 2021.

case: *Mr. P. Sharma and Mr. Ors v Satish Chandra*[2] (District Magistrate), Mr. Delhi and Mr. Ors where such warrants are issued for such hunting and seizure under the CRPC section 94 and 96. The Supreme Court concluded that any searching intensity and seizure did not repudiate the divine order. In addition, by its perceptions as under: the effect of such a search and confiscation in any arrangement of law, which has the abrogating capacity of the State to insure social security, a force essentially administered by law, had ceased to give recognition to the privilege of protecting the essential right guaranteed by the Indian Constitution.

When the constitutionalists saw that, by recognition of a fundamental right to security, which was practically equivalent to the Fourth Amendment, such guideline should not be exposed to any established impediments, then we do not have a legitimacy to import it into a totally special central right, through some procedure of underlined development. Nor is it genuine to agree that legal procedures for sight would be overcome by the sacred insurance under Article 20(3).

In such an example the *State of Uttar Pradesh and Ors vs Kharak Singh*[3]. The problem which the Supreme Court should be considered was if, on the basis of Article 21 of the Constitution of India, recognition by house visits of the accused around dusk was an abuse of the right which raised the matter of whether Article 21 had been completed for the right to protection. The Supreme Court found that, in contrary to Article 21, if such recognition is true. Moreover, most of the judges held that Article 21 could not be construed in any basic right without reserve or explicitly cover any protective measure in accordance with this right to security.[4]

The IT Act 2000 principally aimed at ensuring that e-commerce was recognized legally in India. Because of this, most regulations address largely the establishment within the country of digital certification processes. In the act, cybercrime is not a term. It only examined computer-related crimes with few examples.

The amendment to the Information Technology Act entered into force in February 2009 with the presidential assent comprises the following important features:

- New amendments were introduced in Section 43 of the IT Act, 2000, in order to allow any person to pay damage to that person to the tune of five crores for the first time any person dealing with sensitive personal information does not have adequate controls that result in a wrongful loss or wrongful gain.
- Article 66 is revised so as to include crimes punished in accordance with Section 43 that have also been modified so as to cover crimes as set out above, and penalties that may extend to three years or to a fine of five lakh or both. This is a change from a previous position where manipulation of an account by introducing the virus was penalized for the first time by prison.
- Whilst this has not been clearly addressed, the requirements referred to here in Section 66 A could construe this. By sending threats, bothersome messages and misleading information about the origin of the message, up to three years in prison has been penalized with fine.
- Added newly Section 66B has been introduced to address the dishonest reception of stolen computer resources and retention thereof. This was likewise penalized with a lakh rupee or both for three or two years.
- Distrustful use of the digital signature of anybody else has been penalized by a prison term of up to three years, and may be subject to a penalty for one lakh's rupees.
- Computer cheating has been penalized with a term of imprisonment of any sort extending up to three years and also with fines extending to one lakh rupee (Section 66D).
- The new section 66F refers to cyber terror actions which undermine India's unity, integrity or sovereignty or which harm people or any part of the people:

1. Denial of service to the nation's resources.
2. Try to enter, access or exceed permitted access to a computer resource.
3. Introduction or introduction of any computer contaminant likely to result in death and injury to or destruction of or interrupted property or to know that the contaminant is likely to cause damage or interference of the essential supplies and services for the life of the community or,

[2] *Mr. P. Sharma and Mr. Ors v Satish Chandra*, 1954 SCR 1077.

[3] *State of Uttar Pradesh and Ors vs Kharak Singh*, 1964 SCR (1) 332.

[4] Rishabh, 'A critical analysis on Data Protection and Privacy Issues in India' *Legal Services India,*<http://www.legalserviceindia.com/legal/article-2705-a-critical-analysis-on-data-protection-and-privacy-issues-in-india.html> accessed 29 August 2021.

without authorization or over-approval, to inadvertent or deliberate access to a computer resource The data or computer database restricted for reasons relating to the security or foreign affairs and any restricted information, information or computer databases, may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the Security of the State or to the Computer database so obtained. The acts were fined by jail, which might lead to life imprisonment. The new phenomenon in India is cyber terrorism. In places such as Ahmedabad, Delhi, Jaipur and Bangalore, the 2008 serial blasts were investigated with a significant amount of evidence of cyber-terrorism; in 2008, there were cyber-terrorism traces at the Mumbai Taj hotel, which is now renowned as 26/11; and the 2010.

- The introduction of inspectors as investigating officers for crimes outlined in the Act was a major development (Section 78). Earlier such inquiries were only carried out by an officer of the deputy police superintendent's rank who was a severe limitation, largely due to the restricted number of officers. With this change, you can expect further cases from the police to be filed and probed.
- All cases involving a penalty of three or more years were recognizable. Offenses having a penalty of three years were also rescued (Section 77B). The modification is welcome, however, to ensure that in many cases covered by the IT law, only cyber terrorism cases, children's pornography cases and infringements by intermediaries are available.
- The Government is further strengthening the extent of the 2000 version, including interception and monitoring, to compact cyber terror, with drastic measures, Section 69 of the IT Act 2000 revised. This was an important alteration in the section, which also enables the government to monitor not only traffic but also to restrict any website via an intermediary. The intermediary shall be penalized by seven years in any failure and shall also be liable to a fine (Section 69(4)). No fine was mentioned earlier in the provision.

SHORTCOMING IN THE INFORMATION TECHNOLOGY ACT, 2000

Although the Act has succeeded in defining the regulatory framework for cyberspace and answers some urgent concerns about technological abuse, it is subject to a number of major gaps that have not yet been addressed. Many experts, like the lawyer of the Supreme Court and the cyber rights campaigner Pawan Duggal claim that the law is toothless law, which is not fully effective in punishing or punishing perpetrators who choose to use cyberplace inappropriately. Some problems of cyber law[5] need to be addressed.

- **Spam**

Unwanted Bulk E-mail may be defined as spam. It was initially considered to be merely an annoyance, but today poses severe economic problems. Strict legislation is needed to deal with the spam problem in the absence of appropriate technology protection. Spamming is not the topic of the Information Technology Act. Anti-spam law is enacted by the USA and the European Union. In truth, Australia has highly strict spam regulations that allow spammers up to $1.1 million per day to be penalized.

- **Phishing**

Phishing, by disguising itself as an entity trustworthy in electronic communication, constitutes a criminal fraudulent procedure of seeking sensitive information, such as usernames, passws and credit card details. Phishing is usually done by e-mail and consumers are frequently asked to enter their personal and financial information on a site. Phishing is an example of a tactic used to trick users of social engineering. In the Information Technology Act, there is no rule on phishing through fraud in the Indian Penal Code, and the action of phishing is not enough to be checked. The customers of State Bank of India recently experienced a phishing assault using an SBI clone. Even SBI did not inform its clients, what is worse. The hour is therefore a law prohibiting phishing activities in India.

- **Internet Banking**

Data protection regulations are intended primarily to protect the interests of those whose data are handled and processed by others. Internet banking involves many third parties, not only the banks and their consumers. Banks have multiple changes of hand in information regarding their clients, transactions etc. Banks cannot rely on their own computer networks for information. The prevention of data leakage or manipulation requiring proper legal and technical protection involves high risks. India has no data protection legislation to leave a law alone that covers such a specific subject as data protection in electronic banking.

The IT Act speaks of illegal access, but it is not concerned with preserving the integrity of client

[5]Parthsarthy&A.S.Pati, 'I.T. Act Its Strength and Short Comings, Overview and Suggestion for Amendments - Information Technology Act' *Legal Service India <https://www.legalserviceindia.com/articles/itact.htm>*accessed on 30 August 2021.

transactions. The act makes banks no obligation to protect customer and customer information. U.K has a data protection law implemented 10 years ago in 1998 that makes banks or anybody holding sensitive information accountable for damages if it is not adequately protected from data. In India, liability for the bank would emerge from the contract because the matter is not governed by any statute.

- **Privacy Protection**

Data security and privacy are major issues that today need to be addressed, since in personal, business and business field's information technologies are of greater relevance. When the data or information is transmitted outside its jurisdiction, the European Union and the United States have rigorous policies concerning the privacy and protection of personal data.

It should also be noted here that the lack of a dedicated privacy law in India has led to a loss of significant foreign investment and other economic prospects. This shortfall has also hindered the true growth of electronic trade[6]. So, it is of paramount necessity to have a statute dealing with various privacy-related concerns today, if not a whole act could be implemented, at least certain aspects regarding privacy and data protection should be included in the Act.

- **Identity Theft**

Identity robbery is a developing concern throughout the world. This problem is failing in IT Act 2000. This is a serious problem, given that India wants corporations in India to ensure that there is no identity stealing in the majority of its outsourcing activity. In reality, identity theft was one of the main reasons for a big occurrence in which UK clients and the Indian web marketing company were informed of their personal details.

- **Cyber War**

Nor was it considered in the Act on the question of cyber war. In accordance with the international law framework, international law is an important aspect of every legal system and necessary regulations must be adopted. In recent times India has been confronted with a lot of cyber strikes from China, and Chinese hackers have overturned Indian firewalls such as a Mongolian rampaging army. In the attacks 26/11 the terrorists from neighboring countries which conspired against India received some classified info as an intellect. The law does not provide for the perpetrators to be held responsible for their action.

The most rampant "*misuse*" internet a person makes today is the download of films via peer-to-peer networks. This infringement of copyright rules is rampant, but the number of offenders is so huge that it cannot be effectively curbed. In order to minimize the growing threat of cyber-crimes by measures, website access is regularly blocked. This was considered a harsh action and infringement by Article 19(1)(a)of freedom of expression and expression.

It is difficult to prove that the offence has been committed because there is no definition of the word "*due diligence*" and "*lack of information*" in the Act. Unfortunately, the Act does not include the enforcement of extraterritoriality. The Law, which came into being to examine cybercrime as an international issue, has no territorial limitations, fully disregards that aspect.[7]

INDIA ON GDPR FOR DATA PROTECTION LAW

Although the EU has recognized the right to personal data protection for a while, India still does not have cross-cutting data protection law (under the Treaty on the Functioning of the European Union). The 2000 IT Act largely regulates cybercrime, and internet intermediaries' responsibilities such as social media platforms, but does include certain protection provisions. In Section 43A, for example, compensation is provided for damages caused by the lack of adequate security standards for protecting sensitive personal information. However, only a patchwork of sector-specific legislative regulations will cover data protection and secrecy obligations.

In August 2017, under Article 21 of the Indian Constitution, the Indian Supreme Court recognized the right to privacy as part of the fundamental right to life. It stated that information confidentiality constituted part of this privacy right and stated that confidentiality included the right to preserve the personal identify. This meant that the patchwork approach to privacy included into existing legislation was not adequate and that a more comprehensive approach to information privacy was needed.

[6]HarisZargar, 'India's Information Technology Act has not been effective in checking cyber crime: Expert' *DNA India* (April 03 2021, 10:48 am) <https://www.dnaindia.com/technology/report-india-s-information-technology-act-has-not-been-effective-in-checking-cyber-crime-expert-1818328>accessed on 30 Aug 2021.

[7]Soumik Chakraborty and Sridhar Kusuman, 'Critical Aparaisal of Information Technology Act' *Lawctopus,* (Dec. 17, 2014) <https://www.lawctopus.com/academike/critical-appraisal-information-technology-act-2000/> accessed on 30 August 2021.

The decision observed that the DPC was previously set up by the Indian Government and that its own authorization was actually given to the functioning of the Committee. However, although the DPC has assessed various legislative structures in other nations to protect privacy, it has decided to submit a draft based mostly on the GDPR.[8]

A number of DPB characteristics demand firms to adapt their business structures, operations and philosophies. A number of others increase expense and complexity for operations. The questions we ask serve as an overview of what companies have to take into account in the new law of India and the increase in data protection regulations worldwide. Understanding these concerns will assist digital organizations to plan ahead, to deal with future restrictions and to decide if specific markets should enter or leave.

In 2017, the Indian Supreme Court determined that the rights of Indians to privacy are constitutional. But, while travelling in the digital world, every citizen leaves a visible trail of data. By controlling the gathering, security, storage, sale and exploitation of this data, DPB wants to secure and protect citizens' privacy rights. New laws would influence cost-benefit analysis for many digital enterprises that typically lose money in providing free services, but which hope to profit from the sale and use of clients' personal information.

- **Consent of the User**

Before collecting their personal data, DPB mandates that a digital enterprise acquires explicit permission from the user. To accomplish so, the scope and the objective of data collecting must be explained. At every stage of subsequent data processing, explicit authorization shall also be obtained. Compliance with this requirement may be difficult, as digital organizations are also processing data to create new data that does not fall under the original user, rather than collecting personal data.

- **Personal Data Ownership**

DPB suggests, in theory, that the data provider own personal data. Although simple, this concept could place an immense strain on digital organizations implementation. A property owner might request the return of his property in the physical world. Digital companies should figure out how to meet this criterion when the user requests that their personal details be erased or retracted from a digital company, for example if someone wants the removal of all their information after they stop being a member of Facebook. Digital enterprises should also go beyond the use and storage of their own data, because they could have sold the information to a third party.

- **Classes of Data**

Three data categories from which a primary can be identified were identified by the DPB: Information on finance, health, sexual orientation, genes, transgender status, caste and religious beliefs are included in sensitive information. Critical data contain information which the government occasionally stipulates to be of extraordinary importance, such as national security or military data. The third category is a broad category that is not specified. For storage and processing of each data class, DPB defines particular conditions that data trustees must fulfil. The servers in India must store all sensitive and essential data. Sensitive data can be processed externally, but must be returned for storage in India. There is no way to remove critical information from the country. There are no broad data restrictions. Currently, digital firms work in a smooth cyber world, where their data are mainly stored and processed economically. The local split proposed by DPB could impose additional costs on digital enterprises, lead to sub-economical storage and processing capacity, and could lead to a breakup of global digital supply chains or so-called "*splinternet*."

- **Sovereignty of Data**

In order to preserve the national interests, DPB maintains the right to access data kept locally. This means that the DPB handle the data of residents as a national asset, not unlike controlling the physical properties of citizens. DPB varies from GDPR in this regard, which does not impose local storage or preferred access for national interest's data. Digital enterprises currently own data as long as they are able to handle privacy concerns and meet the conditions for user acceptance.

- **National Interests**

In several circumstances, the DPB does not respect privacy rights while putting great focus on the privacy of residents. It specifies that "*Part government agencies in the processing of personal data shall not be subject to all or any of the provisions of this Act...*" In other words, numerous governmental bodies in India will not require individuals to have the permission to collect their personal information in response to State safety, identification of illegal activities or fraud, and medical and epidemic emergencies. Digital corporations could request these data. The government may also order the supply of

[8] Anirudh Burman, Will a GDPR style data protection law work for India, *Carnegie India*, (May, 15, 2019), <https://carnegieindia.org/2019/05/15/will-gdpr-style-data-protection-law-work-for-india-pub-79113> accessed on 30 August 2021.

non-personal or anonymized information to a digital corporation for research or planning purposes. Critics worry that government may misuse these data for unintentional purposes like political monitoring. Others say that it is easy to deanonymize anonymous data. In order to meet these standards, digital companies may need to adjust their practices.

CONCLUSION

The Information Technology Act (Amendment) of 2008 is an appropriate case study for the analysis in the field of cybercrime legislation of law-making and policy formulation which clearly shows the need for carefully worded provisions; foresight in drafting and imagination with regard to explanations for certain sections. The inadequacies of the legislation and the resulting realistic expectations reinforce the idea that criminal law cannot be left open to wider interpretations, particularly with regard to internet regulations, given that cyberspace provides certain freedoms of action that make it easier to break the law and with such environmental characteristics. Although the aim of the Act on IT was to deal with increasing trends in cyber-criminality and to make it difficult to be cyber criminals, the irony lies in the fact that what was eventually brought into being by the Act is a situation in which it may not be "*easier to be a criminal*", but rather '*easier to be classified as a criminal*.' There can be no overemphasis on the risk in both circumstances.