# THE EVOLVING REGIME OF CYBERSECURITY IN INDIA: AN INTRODUCTION

**Bilal Ahmad Ganai**
Assistant Professor of Political Science
Department of Law, School of Legal Studies,
Central University of Kashmir, Ganderbal, Jammu & Kashmir, India.

***Abstract:*** Cybersecurity is becoming important in the modern world today as technology is opening up new ways of integrating the world and the emergence of cyberspace is reinventing the planet. The emergence of cyberspace is giving rise to new challenges not only for the administrators but to law makers as well. The technological changes are taking place at such a speed that law sometimes fails to keep pace with these developments. If the regulatory compass of the law makers is not broader enough to negotiate these developments, there are chances of these technological developments not working to the advantage of the people. This article analyses legal and policy measures taken by the government at different periods of time on cyber-crimes and scans India's cybersecurity journey from its inception to some of the modern developments. I have followed a descriptive approach regarding the various developments in cyber-security in India.

***Index Terms*** **- Cybersecurity; Data Privacy; Cybercrimes; and Technology.**

## INTRODUCTION

Cyber security is becoming increasingly important nowadays, but the complexity of this concept cannot be overlooked. Cyber security is a multifaceted term that encompasses the practices and processes we use to protect our cyberspace. During the Covid19 the entire world was forced to go online. The threat posed by Covid19 enhanced the online transactions. When the Covid-19 virus forced people to stay at home, the entire world had no choice but to be safe in their homes and take measures for organizing their day-to-day affairs online. While many people were blessed to have these digital facilities available, there were others who had no clue what this online world was going to be all about. This sudden transition represented a massive, unplanned social experiment, accelerating the integration of technology into the fabric of daily life and creating new sociological paradigms.[1]

This development led to the transformation of the entire world, wherein the cyberspace was established as an important part of a human being's life. This development also fed into the emergence of e-commerce, which was a totally different phenomenon.[2] Accordingly, the e-commerce market thrived, and the emergence of Edutech companies, especially in the education sector, was also a path-breaking development.

Cyberspace is a unique ecosystem consisting of interactions between people, software and services, supported by the worldwide distribution of information and communication technology (ICT) devices and networks.[3]

Cyber space is not a physical space. It is a virtual environment where people interact with each other through online communications, transactions, or exchanges. In this way, cyberspace is very intangible in its nature. The internet has led to many changes. For example, the concept of territory, as it was operational earlier, has undergone a tremendous transformation. In fact, the question of territorial jurisdiction has become complicated largely due to the fact that the internet is borderless. There are no physical borders between one region and another in cyberspace. The computer, as a physical object stores the information. This stored information in computers has created the cyberspace, where information is held and transmitted to and from the web. Therefore, the question of where this information is held is one of the important issues that many researchers have raised.[4]

Cyberspace has been created through computers and computer-generated networks. It is an information driven space and it is far more powerful in terms of scalability than the physical space. Meaning thereby it has a global appeal and the quantum of impact that cyberspace has is far larger than the physical space. But as true with every human interaction in this world, it is not immune from problems. If left unregulated and unsupervised it can land people in dangers at the hands of other human beings and groups. Scalability of cyberspace thus feeds into the scalability of cybercrimes.

For example the crime like theft does not necessitate any more the physical presence of the person who wants to commit the theft and the person on whom he wants to commit the theft at one single place. The emergence of smartphones, Internet of Things (IoT) devices, Cloud storage & Online accounts, Social Media, Public Wifi apart from making the life of people easy and more resourceful has equally converted them more vulnerable to cybercriminals who leave no stone unturned in taking every opportunity to harm them by stealing their data or sensitive information even when they are hundreds and hundreds of kilometers away from them.[5]

For example we have recently seen the rise of what has come to be known as the phenomenon of vacation burglaries. For example in 2017, in the industrial district of West Burdwan in West Bengal burglars targeted the locked homes by checking travel relating postings and photographs that the residents had shared on social networking cites. “Though we have tracked the modus operandi of the tech-savvy burglars, we have been unable to nab the culprits due to their discreet operation and due to jurisdiction limitations, as most criminals slip into safe houses in neighboring Jharkhand after every burglary. Hence, we have started making announcements over loudspeakers, and at fairs and festivals, urging people not to post their travel plans on Facebook, or even post photographs from their vacation spots,” a senior police official said.[6]

### UNDERSTANDING CYBERSECURITY: CONCEPTUAL FRAMEWORK OF CYBER SECURITY

Cybersecurity has been debated by jurists mainly from two theoretical lenses. One category of thinkers known as cyber libertarians strongly advocate for the minimum restrictions by the government agencies on the cyberspace. They argue for the maximum freedoms for the people. Their point of view is that internet should remain a free-space. They believe in the liberating

power of the free cyberspace. They are the votaries of strong privacy rights of the individuals. This perspective champions a vision of the internet user as an autonomous agent, whose personhood and capacity for self-determination must be protected from external interference.[7]

John Perry Barlow who has written A Declaration of the Independence of Cyberspace (1996) is one of the main faces of cyber libertarianism.

They strongly disapprove of the regulatory measures of the government for fixing the cybercrimes instead they believe in the use of technological measures that is technical design for eradicating the cybercriminals. Instead of banking on the laws for the protection of internet users, they talk about perfecting the codes so that potential cybercriminals are unable to harm the interests of common people who live in the cyberspace. Accordingly they emphasize on the empowered individuals, privacy-enhancing tools (PETS), and minimization of regulatory might of the state.

The European Union Agency for Cybersecurity defines pets as technologies that embody fundamental data production principles by minimizing personal data use, maximizing data security, and empowering individuals. So far as these technologies are concerned, they take various forms. Some of these forms are as follows: Anonymization, pseaudynomization, data masking, tokenization, encryption etc.

Cyber libertarians thus propose the use of what Paul De Hert & Serge Gutwirth [8] has termed as opacity tools which protects individuals against the state interference. The philosophy of opacity tools can be understand by the philosophy of the first generation of human rights. The first generation of human rights advocate for a very strong private sphere which is impenetrable when it comes to the powers and functions of the state. They thus recognize the opaque nature of individuals.

As per this school of thought the recognition of private sphere led to the emergence of autonomy and self-determinaton rights. They propound a negative relationship between the powers of the state and individual liberties. For them the rise in the powers of the state leads to the decrease in the rights of the individuals. The tool of opacity determines as zone of non-interference and a good example is the protection of the 'sanctity' or inviolability of the home. This concern revolves around the respect for individual autonomy: public authorities (but also other citizens) must respect the bounds of the home.[9]

On the other hand, there are those who subscribe to the cyber paternalism which is an opposite of cyber-libertarianism. They believe in the vibrant role of the government in sanitizing the cyberspace in such a way so that potential cyber criminals are held at bay. Accordingly strong centralized control and regulation is considered as important for the safety of residents of the cyberspace. Accordingly surveillance and censorship rights of the government are considered as important line of action for the state and government.

However this centralized control in a democratic constitutional state demands the use of transparency tools rather than the opacity tools. The transparency tool becomes important so as to not let this surveillance and censorship derail into what many jurists have termed as digital authoritarianism. The transparency tools take care of the principles of the democratic constitutional state which emphasizes on checking the powers of the government, not by drawing the limits of their reach through the recognition of a private sphere of autonomy, but by devising legal means of control of these powers by the people, by controlling bodies or organizations and by other state powers.[10] Thus rather than restricting the powers of the state, we have to channel the powers through the transparency tools.

## LEGAL AND POLICY EVOLUTION: HISTORICAL DEVELOPMENT OF CYBERSECURITY LAWS IN INDIA

### Information Technology Act – 2000

The Information Technology Act was created in 2000. The main focus of this act was to facilitate the growth of electronic-based transactions, to provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer-based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide.[11] It punishes various cybercrimes relating to computer resources, including dishonestly or fraudulently accessing a computer resource without the permission of its owner.

Under the old act, criminal offences were specified under sections 65, 66 and 67 of Ch. XI ("Offences"). The provisions were broad in scope and encompassed typical cyber-crimes without specificities. With the introduction of new offences under the Amendment Act in 2008, there are a host of differentiated offences that have criminal penalties attached to them. The new offences range from sending of offensive messages, hardware and password theft to voyeurism, pornography and cyber terrorism, which have been inserted through amendments to sections 66 and 67 of the IT Act, 2000.[12] In addition, the civil wrongs set out under section 43 of the IT Act have now been qualified as criminal offences under the ITAA 2008, if committed dishonestly or fraudulently.

### Group of Experts – 2011

This group was formed in 2011 and Justice A.P. Shah was nominated as its chairman. This group recognized the importance of the safety and privacy of the personal information of the individuals. It identified certain important principles for the protection and security of the individuals in the cyberspace which came to be known as Nine Privacy Principles.

### National Cyber Security Policy (NCSP) – 2013

This policy got formulated in 2013 with a vision to build a foolproof and vibrant cyberspace for all the stake-holders citizens, businesses and government. One of the important objectives of this policy was to create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.[13] In order to achieve these targets it envisaged to establish a National Nodal Agency for coordinate all matters related to cyber security in the country, with clearly defined roles and responsibilities. It emphazied on a strong regulatory legal framework to address the cyber security challenges arising out of technological developments in cyber space like cloud computing, mobile computing, encrypted services and social media.

### National Cyber Coordination Centre (NCCC) – 2013

National Cyber Security Coordinator (NCSC) under National Council Secretariat (NSCS) was established in 2013 to coordinate with different agencies at the national level for cyber security matters. This Centre evolved a multipronged strategy for the prevention of cybercrimes and continuous updation of the cybersecurity related laws. As cybercriminals are continuously on the move to innovate for perpetrating the cybercrimes, there is a need to constantly monitor the legal landscape so that we are able to eliminate the outdated laws. However given the break neck speed of cybercrimes and deepening of cyber space, the system has not been able to negotiate with the increasing number of cases.

**Justice B. N. Srikrishna Committee & the Draft Personal Data Protection Bills – 2017**

Ministry of Electronics and IT (MeitY), Government of India, on 31st July, 2017 constituted a committee on the protection of personal data of the individuals. On the basis of the report of this committee a Draft Personal Data Protection Bill (Draft PDP, 2018) was drafted which formulated the various principles and doctrines for the safety of personal data in India. This committee submitted their report after studying the established and well-known data protection regimes across the world. The revised version of this Draft Bill was introduced in the lower house of the parliament in 2019. This Bill has been referred to a Joint Parliamentary Committee for an examination.

From the above, we can easily conclude that as far as the issue of cyber-security in India is concerned, it has received a lot of attention in recent years. Many government bodies and institutions have taken a keen interest in discussing this issue and making decisions on securing and protecting cyberspace. This is not an exception found only in India; in fact, all countries across the world are increasingly debating and discussing the nuances and intricacies of cyber-security-related issues, both at the technological level and at the legal level.

## JUDICIAL DEVELOPMENTS IMPACTING CYBERSECURITY

Judiciary in India has decided many cases related to the cyber security issues. All these cases have helped in the development of cybersecurity related jurisprudence in India. Some of the prominent cases that we can refer to are as under:-

**State of Tamil Nadu v. Suhas Katti (2004)**

This case [14] dealt with online harassment and obscenity in India. The conviction was done under section 67 of the IT Act along with other relevant provisions of the law. It involved the Yahoo message group. In this case the accused was sending defamatory and obscene messages in the name of the victim a woman.

**Avnish Bajaj v. State (NCT of Delhi) (2004) – Safe Harbor Principle**

This case is also known as Bazee.com Case. [15] Its jurisprudential value lies mainly in interpreting the doctrine of intermediary liability of the IT Act and how that led to the development of cyber law and criminal liability of corporates in India. It developed the idea of active knowledge or involvement and differentiated it from facilitation via a platform. It led to the development of 'Safe Harbour Principle' under section 79 of the IT Act (amended in 2008) which talks about certain situations wherein intermediaries cannot be held strictly liable if they have followed certain due diligence.

**Syed Asifuddin v. State of Andra Pradesh (2005)**

The jurisprudential value of this case [16] is in its granting of legal protection to the embedded software of cellphones. It was a path-breaking development and resulted in the expansion of the meaning of the term 'hacking'. It also recognized the IPR value of the embedded mobile software.

**Shreya Singhal v. Union of India (2015)**

In this case [17] the vagueness & misuse of the cyber security law section 66A of IT Act was under discussion. It calibrated the Freedom of Speech & Expression as enshrined in the constitution as per the demands of the emerging digital sphere in India. The terms that section 66A of the IT Act had incorporated in itself were open-ended and it led to the unlimited powers in the hands of authorities who misused it for suffocating the free debates and discussions on the digital public sphere. Actually the jurisprudential clarification around the terms like discussion, advocacy and incitement was in so many ways enlightening. This judicial action underlines the critical importance of precise language in law, a philosophical concern that echoes debates in the philosophy of language about how the meaning of words is derived from their use.[18]

**Justice K. S. Puttaswamy and Another v. Union of India (2017)**

In this case, the Supreme Court of India unanimously ruled in 2017 that privacy is a fundamental right.[19] The right to privacy is protected as an intrinsic part of the right to life and personal liberty, as part of the freedom guaranteed by Part III of the Constitution. The right to privacy is inherently protected under Article 21. However, the right to privacy is not absolute and is subject to reasonable restrictions, like most other fundamental rights.

In its judgement SC treated informational privacy as one of the important components of the right to privacy. It was this component which dealt with the rights of citizens in the cyberspace. This landmark judgment on privacy has had far-reaching implications, forming the bedrock for subsequent legal challenges and social activism in the digital age, including those related to identity and expression.[20]

**Google India Pvt. Ltd. v. Visakha Indutries Ltd. (2018)**

In this case Visakha industries accused google of facilitating a defamatory article against it and is liable for the same. This case that way also dealt with the availability of safe harbor principle to google. i.e., section 79 of the IT Act. In this case the court elaborated on the conditionality of the Safe Harbor Principle. It led to the strengthening of accountability of the intermediaries in India.[21]

So, from all the cases that we have discussed above, we can see how the judiciary has played a proactive role in dealing with various cybersecurity-related issues in India. The activeness of the judiciary in responding to these challenges that technology has presented to society is praiseworthy. However, given the dynamism of technology, which makes it elusive due to continuous upgrades, innovations, and inventions, courts in India need to remain vigilant against new technologies. This means that while many things have been accomplished, there are still many other actions we need to take in the future.

## EMERGING CHALLENGES IN CYBERSECURITY

Although there are many things that we have done so far regarding legal responses and other institutional responses, there is still a long way to go when it comes to creating a safe and secure cyberspace in India. One of the important challenges concerning the security of cyberspace for citizens is the widening and deepening of internet-related facilities in the country. E-commerce and the digital economy are becoming realities, and citizens are increasingly taking an interest in the digital public sphere.

With the expansion of the digital public sphere, the cybersecurity of citizens will always be a challenge. How we will be able to address this challenge, given the increasing pace of digitalization of our individual and public spheres, is something we must consider.

Well, as far as the Telecom Statistics India 2019 report is concerned, the overall tele density across India is 90.1%, which is approximately 90 telephone connections per 100 people. According to this report, rural tele density is 57.5%, meaning there are 57

connections per 100 people in rural areas, while urban tele density is 159.66%, indicating more than 1.5 connections per person in urban areas.

This data suggests an important divide between rural and urban tele density and indicates the rampant use of cell phones and telephones by the people in India. Day by day, tele density is on the rise, meaning the population of cyberspace in India is continuously increasing.

This increase in the population of cyberspace in India presents significant challenges to law enforcement officers, as crimes that were previously occurring in the physical public sphere are now being perpetrated in the digital public sphere. The scalability of these crimes is far greater than that of crimes in the actual physical world.

These developments should ring alarm bells for lawmakers and law enforcement officers. The response to these emerging challenges cannot solely rely on the regulatory frameworks of government agencies; it also equally rests on the shoulders of programmers, innovators, and technocrats. They are expected to create and program technology and electronic gadgets in such a way that the code they develop serves as a shield against potential cybercrimes.

## WAY FORWARD

Deepening of cyberspace holds immense potential for the people, but at the same time, the problems that it will unfold for them should be carefully debated and discussed. Furthermore, the increasing sophistication of cyber technology also raises multiple challenges for the lawmakers and law practitioners. No piecemeal approaches will suffice to deal with cybersecurity-related problems, given the burgeoning complexities in this area.

As cyberspace is extraterritorial because internet is not limited to any one country, there are multiple challenges that we have to negotiate while conducting cybersecurity related investigation when any cybercrime takes place. The lack of technical expertise to deal with anonymity and encryption and jurisdictional conflicts are some of the biggest hurdles that come in the way of ensuring a secure cyberspace for the masses.

This problem can be resolved by ensuring that the various countries are proactive about active participation in tailoring treaties for the prevention and cure of various cybercrimes. Any isolationist approach on their part will only work to their disadvantage. After globalization, the emergence of cyberspace is another important force which is going to further integrate the word.

Given all the issues concerning the current cyber security regime in India, there is a significant need to establish an authority similar to what we have in European Union like European Data Protection Board and National Data Protection Authorities so as to take coherent measures of the safety of citizens in India. This authority would supervise, coordinate, and regulate all cyber security and data security-related issues and concerns in India.

We have already established similar authorities in other sectors, but with regard to data protection, we have yet to create a fully-fledged independent autonomous authority to address the issues in this particular area.

## CONCLUSION

The response to cybersecurity-related problems in India has not been proactive. However, we have seen many important developments at both the legislative and judicial levels regarding the development of jurisprudence related to cybersecurity issues. Still, there is a lot that needs to be done. Unless the government mainstreams its focus on cyber security issues in India on a full scale, we won't be able to develop laws regarding cyber security in the best possible way.

The response to the challenges of cyber security must be strong and comprehensive. We need to continuously revisit the existing laws regarding cyber security to ensure that recent technological breakthroughs are factored into the law-making process. The amount and speed of change that technology brings to society is truly challenging. The development of e-commerce and the digital economy, along with the increasing challenges it poses to law-making agencies regarding regulatory aspects, are very important and serious.

With the rise of AI, the concerns regarding the security of cyberspace are becoming more prominent. There are many who speak about the development of quantum AI, which is far superior in its scope and scale compared to classical AI. Apart from quantum AI, the development of the Internet of Things (IoT) also highlights the scope of cybersecurity-related concerns and issues. With the massive digitization that our country has seen, along with the various institutions and official businesses, we are definitely in for a strong transformation. This technology-driven transformation of our society increasingly demands the enhancement of the cybersecurity measures that we need to put in place.

It has also been observed by many stakeholders that the IT Act of 2000, which was a watershed in the development of electronic commerce in India, has now outgrown its relevance. The Act was a legislative response to the IT revolution that promised to be a key driver of India's economic development.[22] Many developments have taken place that have rendered this IT Act ineffectual in addressing various modern-day challenges.

One of the prominent modern-day challenges that the IT Act has not been fully able to address is the protection of data, which is characterized by many people as the modern-day oil or fuel. The rise of the digital economy has significantly increased the importance of data within society, along with the development of the Internet of Things (IoT) and AI. These developments make the IT Act of India less equipped to address the challenges posed by them.

There are many aspects we need to work on regarding the security of cyberspace and the evolution of the best data protection regime in India.

## REFERENCES

[1] Kumar, A. (2013). Social thinking to scientific social theory: An introduction to sociology and social anthropology. *International Journal of Research in Sociology and Social Anthropology, 1*(1), 1–5.

[2] Rajput, M., & Kumar, A. (2019). When pessimistic becomes entertaining: Exploring an added face of online media content. *International Journal of Communication and Social Research, 7*(1&2), 12–16.

[3] Ministry of Electronics and Information Technology. (2013). *National cyber security policy, 2013*. Government of India.

[4] Muralidhar, S. (2010). Jurisdictional issues in cyberspace. *Indian Journal of Law and Technology, 6*, 1–21.

[5] Van Hoorde, K., De Pauw, E., Vermeersch, H., & Hardyns, W. (2018). The influence of technological innovations on theft prevention: Perspectives of citizens and experts. In J. P. Burgess, G. Reniers, K. Ponnet, W. Hardyns, & W. Smit (Eds.), *Socially responsible innovation in security: Critical reflections* (pp. 91–110). Routledge.
[6] Chanda, A. (2017, December 24). Burglars track vacation posts to strike at homes. *The Indian Express*. https://indianexpress.com/article/india/burglars-track-vacation-posts-to-strike-at-homes-4999341/
[7] Kumar, A. (2014). Personhood, autonomy, agency and responsibility: An appraisal of Frankfurt's philosophy of action. *KAAV International Journal of Arts, Humanities and Social Sciences, 1*(1), 202–207.
[8] De Hert, P., & Gutwirth, S. (2006). Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In E. Claes, A. Duff, & S. Gutwirth (Eds.), *Privacy and the criminal law* (pp. 61–104). Intersentia.
[9] Ibid.
[10] Ibid.
[11] Naavi. (2006). *Information Technology Amendment Act 2006: Statement of objects and reasons*. [Blog post]. Retrieved October 1, 2020, from https://www.naavi.org
[12] Mohanty, A. (2011). New crimes under the Information Technology (Amendment) Act. *Indian Journal of Law and Technology, 7*, 103–124.
[13] Ministry of Electronics and Information Technology. (2013). *National cyber security policy, 2013*. Government of India.
[14] *State of Tamil Nadu v. Suhas Katti*, CC No. 4680/2004 (Chief Metropolitan Magistrate Egmore, 2004).
[15] *Avnish Bajaj v. State (NCT of Delhi)*, 116 DLT 427 (Delhi High Court 2005).
[16] *Syed Asifuddin v. State of Andhra Pradesh*. (n.d.). Legal Wires. Retrieved October 1, 2020, from https://legal-wires.com/case-study/case-study-syed-asifuddin-v-state-of-andhra-pradesh/
[17] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (Supreme Court of India).
[18] Kumar, A. (2019). The use theory of meaning: A reading of Wittgenstein's Philosophical Investigations. *International Journal of Emerging Technologies and Innovative Research, 6*(5), 223–226.
[19] *Justice K. S. Puttaswamy (Retd.) v. Union of India*, AIR 2017 SC 4161 (Supreme Court of India).
[20] Kumar, A., & Bendukurthi, N. (2017). The unfinished legal business on (homo)sexuality: A media mapping of LGBT activism in India. *International Journal of Communication and Social Research, 4&5*(1&2), 11–26.
[21] *Google India Pvt. Ltd. v. Visakha Industries Ltd.*, AIR 2020 SC 350 (Supreme Court of India).
[22] Kumar, A. (2011). Economic development in India: A response to the information technology (IT) revolution. *ECONSPEAK: A Journal of Advances in Management, IT & Social Sciences, 1*(1), 105–109.