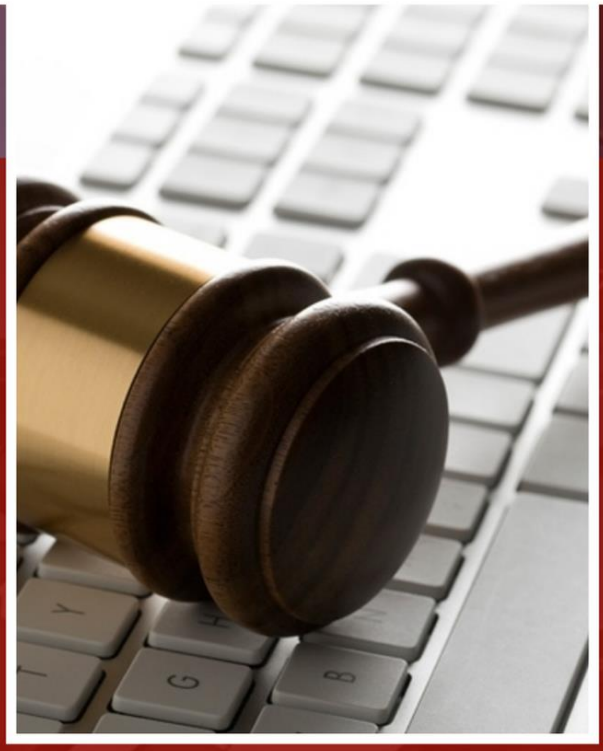
VOL. I/ISSUE I/2021

Cyberlaw University®

Education in Cyberlaw - A cut above the rest



A CYBERLAW UNIVERSITY INITIATIVE

CYBERLAW UNIVERSITY INTERNATIONAL E-JOURNAL

WWW.CYBERLAWUNIVERSITY.COM

EMERGING CYBERLAW TRENDS IN 2021 IN INDIA

- **Abstract**

The year 2021 promises to usher in a new era of cyber legal developments and growth as far as India is concerned. This year is promising to see a plethora of activities which will contribute to evolving cyber legal frameworks and related ecosystem in India.

- **National Cyber Security Strategy**

One of the first keenly awaited trends in Indian Cyberlaw jurisprudence in the year 2021 will be the National Cyber Security Strategy. This Strategy will aim to build on the National Cyber Security Policy 2013 and would aim to be a comprehensive guiding gospel for individuals, all decision and policy makers as well as other stakeholders. The said Strategy is likely to throw more light on appropriate response mechanisms concerning protection of cyber security in all government and other sectors in India.

The Government of India has been working on the National Cyber Security Strategy for quite some time and the entire world is looking up with bated breath to see how the said Strategy is going to evolve. The National Cyber Security Strategy should inform the appropriate relevant authorities of all considerations they need to take into consideration, while dealing with cyber security ramifications concerning their operations. This assumes more significance as India is consistently on the radar as a potential target by cybercriminals and cyber security breaches. Given the fact that India does not have a law on cyber security, the National Cyber Security Strategy should be seen as an interregnum step, before India graduates to a full-fledged cyber security law.

While all attention will be on the new National Cyber Security Strategy, we need to be mindful of the legal ramifications of the said Strategy. The said Strategy document will be the manifestation of Government's thought processes and will not have the statutory penal force behind the same, unlike a law passed by the Parliament. Hence, the Strategy would be only a directory and would no longer be mandatory.

- **Need for Dedicated Law on Cyber Security**

Very quickly, India will have to work start working extensively on coming up with a dedicated national cyber security law. The need for having cyber security law by India is immense, because that will be an important tool to protect India, its cyber security and its cyber sovereign interests. At a time when a lot of other countries have already started coming up with dedicated laws on cyber security, India is slightly behind the curve. There is a need for appropriate action in this regard in order to ensure that India does not lag behind others in this direction.

- **Growing Cybercrimes in India and Their Regulation**

Meanwhile, cybercrime is likely to consolidate its further growth and position ever since the advent of The Golden Age of Cybercrimes in the year 2020. Cybercrimes including phishing, identity theft, and frauds have massively increased in the last one year. However, their coverage under the existing laws are neither adequate nor comprehensive.

We are further likely to see much more growth and consolidation in cybercrime penetration in India. This would underline the need for coming up with more effective and deterrent legal frameworks to regulate cybercrime. Hopefully, the year 2021 would see the Government focusing on more effective ways of trying to combat the newly emerging cybercrimes including phishing, identity theft, and financial frauds. The year 2021 could see the initiation of a process of making more stringent legal provisions for fighting cybercrimes in India. As per one survey in terms of motive, the maximum 60.2% cyber crimes lodged in 2020 were done for fraud (30,142 out of 50,035 cases), the NCRB, which functions under the Ministry of Home Affairs, stated.[1]

- **Personal Data Protection in India**

Another major Cyberlaw trend in India for the year 2021 will be the passing and implementation of the Personal Data Protection Bill, 2019. Historically, India has not had a dedicated data protection law. The Government of India had tabled the Personal Data Protection Bill, 2019 before the Parliament of India in December 2019. The year 2020 saw the said Bill under the active consideration of the Joint Parliamentary Committee of the Indian Parliament.

At the time of writing, it is expected that the said Joint Parliamentary Committee would come up with its report in 2021 and on the basis of the same, the Government is likely to make appropriate changes in the Personal Data Protection Bill, 2019 and have it passed in the Parliament. This Bill is likely to change the rules of the game, in terms of providing stringent obligations for all data handling entities. Implementing the Personal Data Protection law will definitely strengthen the Indian Information Technology ecosystem, apart from strengthening appropriate protection for personal data. Hence, all stakeholders need to be prepared for a new set of compliances concerning data protection in the year 2021.

- **Protection of Non Personal Data in India**

This year is also likely to see the Government coming up with new approaches to deal with the protection of non-personal data. This is important as the Personal Data Protection Bill, 2019 only has a limited mandate of protecting personal data and non-personal data is clearly outside the ambit of the said law. It will be imperative that the Government would need to work extensively on the protection of non-personal data as well.

- **Need for Updating Indian Cyberlaw**

The year 2021 is also expected to see movement towards appropriate amendments in the Indian Information Technology Act, 2000. It is pertinent to note that the Information Technology Act, 2000 is India's mother legislation to deal with all activities in the electronic ecosystem. The said law was passed more than two decades back and only got amended in the year 2008 and has been crying for appropriate amendments to make it more topical and relevant with the passage of time.

It is also hoped that the year 2021 could potentially see more appropriate changes in the Indian Cyberlaw, to incorporate enabling legal provisions to deal with the challenges thrown up by newly emerging technologies.

---

[1]PTI (2021). India reported 11.8% rise in cyber crime in 2020; 578 incidents of "fake news on social media": Data. *The Hindu*. [online] 15 Sep. Available at: https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece.[Accessed 15 Dec. 2021].

Further, the year 2021 is expected to see the Government coming up with new rules and regulations under the Information Technology Act, 2000. This is so because there are various areas and issues, where the Government needs to come up with appropriate rules and regulations under the Information Technology Act, 2000.

- **Protecting Indian Cyber Sovereignty**

The year 2021 should also see activities in the direction of enhancing and consolidating of cyber sovereignty of India. India as a nation needs to give more pronounced focus and importance to cyber sovereignty. India needs to learn from the experiences and experiments of other nations on cyber sovereignty and come up with appropriate mechanisms and processes to protect and preserve Indian cyber sovereignty.

- **Need For More Clarity On Blockchains**

The year 2021 could also hopefully see more action in India in terms of clarity on the legal issues concerning bitcoins and blockchains. India is by and large pretty ambivalent of its legal approaches concerning bitcoins and blockchains. However, with the increased adoption of Blockchains in various sectors of human activities and endeavors, the need has become more prevalent for India to come up with dedicated legal frameworks to regulate bitcoins and blockchains.

- **Enabling Regulation of Artificial Intelligence**

The year 2021 could also see more action in terms of coming up with enabling legal frameworks to regulate Artificial Intelligence. Artificial Intelligence is growing at a very rapid pace. A lot of developments are taking place in various applications of Artificial Intelligence in various sectors. However, the absence of enabling legal frameworks on Artificial Intelligence has led to a situation where enabling legal frameworks are required for further growth of Artificial Intelligence. Hopefully, the year 2021 could also see the Indian Government focusing on enabling legal frameworks for promoting Artificial Intelligence.

- **Enabling Regulation of Cloud Computing in India**

Further, we are likely to see more growth in terms of enabling legal frameworks for promoting cloud computing. As per one estimate in 2022, the Global public cloud infrastructure as a Service market is expected to be worth around 122 billion U.S. dollars.[2]

- **Expanding Scope of Data Breach Notification Law in India**

Data breach notification laws in the country would require a revisit. Hopefully, the year 2021 should see action in this regard. This is so because the data breach notification requirements are of the year 2017. Since the year 2017, a lot of new developments have taken place in terms of emerging varieties of cyber security attacks and breaches. There is a need for expanding the kinds of cyber security breaches that need to be reported, within the ambit of breach notification laws.

---

[2]Statista. (n.d.). *Public cloud IaaS market worldwide 2022*. [online] Available at: https://www.statista.com/statistics/505251/worldwide-infrastructure-as-a-service-revenue/.[Accessed 15 Dec. 2021].

The previous years have seen that the data breach notification laws in India are observed more in breach rather than in compliance. The absence of enforceability of legal consequences for non-compliance with data breach notification laws has further changed the landscape and has pushed the Indian corporates in a level of complacency.

We are beginning to see more non-reporting of cybersecurity breaches, though these breaches have increasingly been reported in the public domain. As per one survey more than 1.1 million cyber attacks were reported across India in 2020. This was a significant increase compared to the previous year's nearly 400 thousand. The country was amongst the top five with the most number of cyber security incidents that year.[3]

Hopefully, the year 2021 would see the Indian Government coming up with more enabling legal frameworks to stringently enforce data breach notification laws in the country.

- **Need for Reviewing Intermediary Liability Provisions**

Hopefully, in the year 2021, the entire aspects of intermediary liability laid down by Section 79 of the Indian Information Technology Act, 2000 is likely to be increasingly coming into focus for potential review by the Government. More and more incidents in the last few years have demonstrated that after the passing of Shreya Singhal v/s Union of India judgment by the Hon'ble Supreme Court of India in March 2015, most of the intermediaries deliberately have misinterpreted the said judgment and taken the role of being a mere spectator, as things go wrong on their networks.

There is an urgent necessity for India to revisit the entire issue pertaining to intermediary liability. The draft Information Technology Intermediary Guidelines (Amendment) Rules, 2018 had sought to put more responsibilities on the intermediaries but it never got to be notified. Hopefully, the year 2021 could also see more action in this regard in the direction of regulating intermediaries.

- **Protecting Indian Critical Information Infrastructure**

India is likely to see far more cyber security breaches in the year 2021 targeted at its critical information infrastructure. Hence, India will have to make special efforts to protect and preserve its Critical Information Infrastructure from potential cybersecurity attacks.

- **Privacy Protection**

With the AarogyaSetu app increasingly collecting humungous volumes of data, Indians silently got sensitized about the need for protecting their privacy. I expect the year 2021 to also see more actions in the direction of having enabling privacy protections in India. As per one survey it was said that the cyber attackers (threat actors) impersonate popular video platforms like Zoom, Google Meet, Microsoft Teams, AarogyaSetu app and WHO to send phishing messages through SMS (smishing), WhatsApp (whishing) or phishing emails to steal identities and engage in other nefarious activities during the COVID-19 pandemic.[4]

---

[3] Statista. (n.d.). *India: number of cyber attacks 2020*. [online] Available at: https://www.statista.com/statistics/1201177/india-number-of-cyber-attacks/[Accessed 15 Dec. 2021].

[4]The New Indian Express. (n.d.). *Phishing attacks in name of Aarogya Setu app increasing: Cyber agency*. [online] Available at: https://www.newindianexpress.com/nation/2020/may/16/phishing-attacks-in-name-of-aarogya-setu-app-increasing-cyber-agency-2144206.html#:~:text=It%20said%20cyber%20attackers%20(threat.[Accessed 15 Dec. 2021].

These are some of the key important Cyberlaw trends that I see on the horizon. Needless to say, I am not a soothsayer or an astrologer as I cannot predict the future. I believe that on the basis of my work, the aforesaid important Cyberlaw trends are likely to impact the growth of Cyberlaw jurisprudence in India in the year 2021.

Looking forward to a very exciting phase of growth of Cyberlaw jurisprudence in India in the year 2021.

- **Bibliography**

1) PTI (2021). India reported 11.8% rise in cyber crime in 2020; 578 incidents of "fake news on social media": Data. *The Hindu*. [online] 15 Sep. Available at: https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece.
2) Statista. (n.d.). *Public cloud IaaS market worldwide 2022*. [online] Available at: https://www.statista.com/statistics/505251/worldwide-infrastructure-as-a-service-revenue/.
3) Statista. (n.d.). *India: number of cyber attacks 2020*. [online] Available at: https://www.statista.com/statistics/1201177/india-number-of-cyber-attacks/
4) The New Indian Express. (n.d.). *Phishing attacks in name of Aarogya Setu app increasing: Cyber agency*. [online] Available at: https://www.newindianexpress.com/nation/2020/may/16/phishing-attacks-in-name-of-aarogya-setu-app-increasing-cyber-agency-2144206.html#:~:text=It%20said%20cyber%20attackers%20(threat.