

INDIAN CYBERLAW DEVELOPMENTS IN 2021

BY

DR. PAVAN DUGGAL
ADVOCATE, SUPREME COURT OF INDIA
PRESIDENT, CYBERLAWS.NET

2021 was indeed a hectic year as far as cyber legal developments in India were concerned. Like the world, India was passing through the era of the pandemic. The year 2021 saw the deadly second wave of infections, which took a lot of toll and towards the end of the year, the dramatic spread of Omicron variant of Covid-19, has begun to start raising a lot of concerns and issues pertaining to its further dissemination.

- **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**

The year 2021 began with some dramatic developments coming from one of majors social media service providers. WhatsApp decided to unilaterally amend its privacy policy and asked all Indians to comply with the said privacy policy if they were to continue enjoying the benefits of WhatsApp platform. Now, the problem with the amended privacy policy was that it effectively cut the hands of Indians. The amended Privacy Policy terms stipulated that the sensitive personal data of Indians, including the transaction data would be shared with a large number of legal entities with whom the user often may not have a privity of contract. The said unilateral action of WhatsApp led to a massive uproar and consequently WhatsApp decided to slightly put the implementation of its amended privacy policy on hold. But this unilateral action of the said service provider had obviously other ramifications.

The government took note of these new developments and on 25th February, 2021 the Government of India notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These rules have been made under section 87 of the Information Technology Act, 2000 and represent secondary legislation under the Indian Cyberlaw. However these rules have been dramatically different from other rules primarily because these rules for the first time provided a deterrent effect and impact in case the intermediaries were not to comply with the parameters of the IT Rules, 2021.

- **Intermediary Liability under Rule 7 of the IT Rules, 2021:**

Two specific instances of legal exposure were provided under Rule 7 of the IT Rules, 2021. Rule 7 stated that if any intermediary fails to comply with the provisions of the IT Rules, 2021, then it will lose its statutory exemption from legal liability which has been granted to them under Section 79 of the IT Act, 2000. The IT Rules, 2021 further stipulated that the snatching away of the statutory exemption from legal liability of intermediaries will be by operation of law. The second more significant legal consequence for non-compliance with the IT Rules was that the top management of the intermediary would be made liable for being punished for various offences under Information Technology Act, 2000 and also under the Indian Penal Code. So for the first time in

the history of Indian Cyberlaw , a deterrent message was given by India to intermediaries that if you don't comply with the IT Rules, 2021 within the statutory period of time, then as an intermediary, be prepared for facing criminal consequences.

By and large, intermediaries have had an extended honeymoon period under the Indian cyber law from the year 2009 till February 2021, because virtually they were asked do nothing, except comply with orders, either from a court of competent jurisdiction or government agency. They were asked to wait on and do nothing pertaining to any third-party data on their network, or on their platform till such time they either got a governmental order or an order from a court of competent jurisdiction. Now that effectively had transformed almost all intermediaries into becoming mute spectators while mayhem was happening on the network, Further, making them liable under the law was not possible because they were given the statutory exemption from legal liability.

Now with the IT Rules 2021 coming in, the colour of the canvas was changed completely and as the year passed we saw that one service provider, Twitter decided to not comply the IT rules within the minimum statutory period that was required for significant social media intermediaries being 90 days. Consequently, after the expiry of the said statutory period, we saw four different FIRs being filed against the said service provider in different states . The net result is that the said service provider is required to answer each of the criminal charges in the criminal proceeding separately and clearly would not have the benefit of the statutory exemption from legal liability that it would have enjoyed, had it so complied with the provisions of the IT Rules 2021. So as we go forward, we been seeing that the government of India is keen to implement in letter and spirit the IT Rules 2021.

Meanwhile, the year 2021 also saw various challenges to the constitutional validity of the IT Rules 2021. Various public interest litigations were filed in different High Courts, challenging the constitutional vires of various provisions of the IT Rules, 2021. The Mumbai High Court did stay a particular portion of the said rules pertaining to digital publishers, but the normal provisions pertaining to intermediaries under Rules 3, 4, 5 and 6 have still not yet been stayed by any court of law. So while the matter continues in different courts, it will be interesting to see how the judiciary interprets the constitutional validity of the IT Rules 2021. But nonetheless the IT Rules 2021 represented a distinctive step forward in India's definitive approach on this entire issue of intermediary liability.

- **Pegasus Judgement**

A lot of litigations were initiated pertaining to issues in Indian cyberspace in the year 2021. The year 2021 saw the Pegasus controversy erupting. In fact, a group of publications and newspapers on a global scale actually came up with an investigation report which stated that the spyware Pegasus was actually being used by different sovereign governments across the world so as to intercept and monitor the activities of various stakeholders in the digital ecosystem. In the Indian context, this particular controversy started having a lot of ripple effects. Various Public Interest Litigations were filed in the Supreme Court and by a historic landmark judgement, the Supreme Court dealt with this entire issue. In the said judgement, the Supreme Court reiterated the fact that the right to privacy is a fundamental right, as has been held by the judgement in Justice

Puttaswamy versus Union of India. The Supreme Court further held that the allegations pertaining to use of Pegasus software have not been controverted by the government and hence it becomes imperative that these allegations must be independently investigated.

Consequently, the Supreme Court appointed a technical committee of experts to look into the various aspects of the Pegasus matter and to give back its report to the Supreme Court. That represents a big step forward as far as judicial review of governmental actions is concerned.

Also, the Pegasus judgement was important in as much as it held that every time the term national security is mentioned by the government, that alone should not be a factor enough for the courts to not consider it. This judgement established the principle that the courts will have the power to go behind the entire issue of national security and national interest and can examine these issues, from the legal perspective. The Pegasus judgment was an important development as far as evolving cyber legal jurisprudence in India was concerned, in the year 2021.

- **Joint Parliamentary Committee Report on Personal Data Protection Bill, 2019**

The year 2021 was significant because in this year, the Joint Parliamentary Committee had been deliberating on the various provisions of the Personal Data Protection Bill, 2019. It is pertinent to note that in December 2019, the Government of India had introduced the Personal Data Protection Bill, 2019. The Parliament had referred the same to the Joint Parliamentary Committee and the committee was deliberating various provisions of the PDP Bill in 2021 and finally on 16 December, 2021 the Joint Parliamentary Committee laid its report on the floor of both the houses of Parliament.

The report of the Joint Parliamentary Committee has by and large, endorsed the Personal Data Protection Bill, 2019, with certain observations. First and foremost, the committee has opined that the ambit and scope of the Personal Data Protection Bill, 2019, was limited as it was only dealing with personal data, but right now given the humongous proliferation of not just personal data and non-personal data, it's imperative that the scope of the proposed law be expanded to refer to a Data Protection Law where not just personal data but also non-personal data can be specifically covered within the ambit of the law.

The JPC also dealt with the most controversial element of the Personal Data Protection Bill, 2019. This was section 35 of PDP Bill which specifically gives the power to the government to exempt governmental agencies from the applicability of the provisions of the Personal Data Protection Bill on certain specified grounds. The said provision was, by and large, upheld by the Joint Parliamentary Committee that held that the sovereign government has indeed the power to go ahead and exempt certain governmental agencies from the applicability of the Data Protection Law.

However, it is important to note that along with the JPC report, various dissent notes were also filed by different members who did not agree with the majority position on this issue of governmental exemptions. Consequently, through these dissent notes, various members of the JPC pointed out that the said exemptions given to government were against the very foundations of Indian Constitution in as much as there would now be two ecosystems. There would be a private

ecosystem of private corporate players who would be required to comply with the parameters of the PDP Bill 2019, while there will be the second ecosystem of governmental agencies and authorities who would be exempted from the applicability of the PDP Bill, 2019. It was further pointed out by the dissent notes that the said approach in itself is in violation of the Constitution apart from negating the very benefits of the Personal Data Protection Bill, 2019.

Now the said report is before the Indian Government, it will be interesting to see how the Indian Government either relies upon or picks up certain elements of the said report and comes up with its own revised version of the Data Protection Bill in the coming times.

- **Crypto-assets and Cryptocurrencies Legal Scenario in India**

It is also important to note that the government of India has been concerned with the entire issues of crypto-assets and cryptocurrencies in 2021. The year 2021 saw Indians increasingly being impressed by the massive increase in value of cryptocurrencies and consequently, more and more Indians started investing in crypto-assets and cryptocurrencies. There were numerous television advertisements by various prominent actors calling upon the innocent Indian users to invest in crypto currencies, without even warning them about the legal sanctity or validity of such cryptocurrencies or crypto-assets.

Consequently, the government stated that it is now going to come up with a Cryptocurrency bill. Earlier, the reported thought process was that maybe cryptocurrency, as a concept needs to be banned, but as subsequent press reports suggested, the thought process evolved and came to a more mature level where it was reported that the government was now keen in the direction of trying to regulate, in an enabling manner, various aspects of crypto-assets and cryptocurrencies.

So, crypto-assets and cryptocurrencies, as an important area of cyber legal jurisprudence, got sufficient attention in the year 2021.

- **Removal of Offending Content on Digital Platforms**

Further, the year 2021, was also significant as the Delhi High Court passed the landmark judgement in the case of “X vs Union of India”. This was the case in which the author was appointed as the amicus curiae by the Delhi High Court. In this particular case, the Delhi High Court upheld the various provisions of the IT Rules, 2021 and specifically mandated detailed processes of how and in what particular manner, steps have to be taken by victims of published online obscene content, as also by the service providers, for the purposes of addressing the various grievances of the said victims.

The said judgement was indeed a landmark judgement and clearly addresses the growing concerns of numerous Indians, across various states, who have been finding themselves becoming victims of all kinds of obscene content being posted online about them. This judgement was indeed historic as it effectively gave effective remedies to victims whose content is either published in the obscene form or whose artificially morphed pictures or images are uploaded on the Internet and also stipulated the mechanism of how these kinds of contents needed to be put down by the service providers in accordance with the IT Rules, 2021.

- **Absence of Regulatory Frameworks Concerning Cybersecurity**

Cyber security was a big area of concern in the year 2021. This was so because India saw massive attacks on its computer systems, networks and communication devices during the pandemic, with under reporting of attacks being the norm of the day.

As more and more Indian companies started becoming victims of ransomware attacks, there was a renewed focus on coming up with new approaches to deal with cybersecurity. But then the year 2021, did not see any effective action as far as cybersecurity legal frameworks was concerned.

It is important to note that India does not have any dedicated cybersecurity law. The Information Technology Act, 2000 is India's mother legislation on the electronic format and though it was amended in the year 2008 to provide a comprehensive definition of the term, cybersecurity, it only had come up with cosmetic provisions pertaining to protection of cybersecurity. Consequently, the Information Technology Act, 2000 is completely inadequate to deal with the challenges of cybersecurity.

Meanwhile, the National Cybersecurity Policy of 2013, remained a mere paper tiger and has not been effectively implemented. There were talks that the government is coming up with the National Cybersecurity Strategy, but the strategy did not see the light of the day in the year 2021. It is expected that in the year 2022, India should be releasing its National cybersecurity strategy.

But from a pragmatic and practical viewpoint, it became very clear that the time has come for India to start taking action. India requires a dedicated national cybersecurity law on the lines of national legislations of other countries who have come up with dedicated national laws on cybersecurity. Till such time we don't have a dedicated law on cybersecurity, we cannot really provide effective remedies to affected persons as far as India is concerned.

The year 2021 once again reiterated the fact that there was a need for amending the IT Act and the various issues and regulations made thereunder.

- **Golden Age of Cybercrime**

The Golden Age of Cybercrime has already begun with the coming of Covid-19. India saw the trinity of Cybercrimes, as the top three cybercrime during the Covid-19 times being phishing, identity theft and online financial fraud. The year 2021 also saw the mushrooming of the Jamtara cybercrime model where small areas, small villages or small communities decided to get together, and dedicatedly work on cybercrime, so that they can get some quick bucks. But the absence of effective legal frameworks to deal with cybercrime effectively marred India's spirited approach to fight and regulate the growing phenomenon of cybercrime.

We also found that the existing provisions under the Information Technology Act, 2000 and also under the Indian Penal Code were completely inadequate to deal with these newly emerging cybercrimes that have emerged in India during the pandemic in the year 2021. Clearly, the time has come that India now must have dedicated legal frameworks for regulating cybercrimes.

- **Need for Data Privacy Laws**

There is a need for India to also address the distinctive vacuum that is currently existing in India pertaining to lack of legislation on digital privacy. India requires a digital privacy law so that the privacy of Indians, both personal privacy as also data privacy, can be effectively protected and preserved in the coming times .

- **International Conference on Cyberlaw, Cybercrime and Cybersecurity, 2021**

Towards the end of year 2021, India hosted the [International conference on Cyberlaw, Cybercrime and Cybersecurity](#) in cyberspace. This is the global go-to conference, which has become an authority of its kind, working on the intersection of cyberlaws, cybercrime and cybersecurity since the year 2014. This year the conference also was able to get some of the top names across the world and saw some very interesting deliberations. Further the conference had come up with its dedicated, detailed outcome document, which elaborated the various recommendations that were given in the 44 odd sessions that took place over three days, with more than 165 speakers from all over the world. The International Conference on Cyberlaw, Cybercrime and Cybersecurity contributes to the growing envelope of cyber legal jurisprudence , at global, regional and national levels.

- **Growing Menace of Fake News**

All said and done, the year 2021, was a remarkable year. It was the year of the pandemic where India saw massive increase in fake news. No wonder pandemic also came to be known as the ‘infodemic’ and because India lacked dedicated law on fake news, it became even more difficult to control the growing menace of Fake News. Some elements of fake news were sought to be addressed under the IT Rules, 2021, but clearly that was not enough. Meanwhile, the entire phenomenon of fake news is continuing to transform the way how disinformation and misinformation is being generated and transmitted by Indians.

- **Consolidation of the Great Indian Vomiting Revolution**

The year 2021 also saw the further consolidation of the growing Great Indian Vomiting Revolution. Indians are vomiting data about their personal, professional and social lives and the year 2021 continued to see the consolidation of this trend. More and more Indians are generating data and given the fact that they're leaving behind their digital footprints indiscriminately, they are increasingly likely to be subjected to a variety of cybercrimes and cybersecurity breaches.

- **Need for More Capacity Building Initiatives**

The year 2021 also brought forward the need for far more focus on capacity building. The Government of India has initiated various initiatives on capacity building, but clearly, they have also to be supplemented by private efforts.

Initiatives like [cyberlawuniversity.com](#) have also been contributing to the growing capacity building on Cyberlaw and related issues. [Cyberlawuniversity.com](#), with whom the author is

associated as an Honorary Chancellor, offers various courses on Cyberlaw, Cybercrime Law, Cybersecurity Law, Artificial Intelligence Law, Blockchain Law and Internet of Things Law. These courses have already been done by more than 27,000 students from 174 countries, speaking 52 national languages. These figures are constantly telling us that the need for capacity building is constantly increasing.

- **Conclusion**

The year of the pandemic, 2021 told us that the future in cyberspace is very promising and yet an uncertain future and hence, the pre-Covid 19 mindset must actually be giving way to more pragmatic and futuristic mindsets. There is an immense need for all digital stakeholders to hone their digital skills so that they can be very well prepared so as to deal with the distinctive challenges pertaining to cyberspace in the future.

All in all, the year 2021 was a very exciting year as far as Indian cyberspace and cyber legal developments were concerned. The Indian cyber legal developments that took place in the year 2021, are going to become the foundation for the further evolution of Indian cyber legal jurisprudence in the coming times. Cyber law, globally and specifically in India, is a constantly evolving paradigm and it will be interesting to watch how new developments will take place in this evolving paradigm of cyber law in the coming times.

The author Dr. Pavan Duggal, Advocate, Supreme Court of India, is an internationally renowned expert authority on Cyberlaw and Cybersecurity law. He has been acknowledged as one of the top four Cyber lawyers in the world. He is also the Chairman of International Commission on Cybersecurity Law. You can reach him at pavan@pavanduggal.com. More about Dr. Pavan Duggal is available at www.pavanduggal.com.