2021 GLOBAL CYBERLAW DEVELOPMENTS

BY

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

Cyberlaw as a legal jurisprudence continues to evolve in the era of the pandemic. The year 2021 was significant as various new cyber legal developments took place, thereby contributing to the growing envelope of Cyberlaw jurisprudence across the world.

Let's examine and highlight some key elements pertaining to Cyberlaw jurisprudence in the year 2021.

Cyber Security As A Matter of Concern

Cyber security continued to be the focal thrust area of concern in the year 2021. Cyber security breaches are the main phenomenon in the year 2021. According to the 2021 Cyber Threat Report by SonicWall, there is a 62% increase in Ransomware since 2019.[1]Pizza delivery service Dominos suffered a massive data breach in May 2021 that exposed order details of 18 crore Pizza orders made via the service. The data breach included 130TB of employee data files and customer details including addresses of the customers. [2]

LinkedIn experienced a number of massive data expose in the year 2021 itself that reportedly affected around 700 million of its users. The data exposed included online and physical addresses, geolocation records as well as inferred salaries of the users and is now up for sale on the dark web.[3]

Further, cyber security legal issues began to start engaging the attention of various governments. More and more governments started engaging in the idea of coming up with national laws on cyber security.

Increasing Cyber Security Breaches

Further, increasing cyber security breaches are one of the key highlights of the cyberspace horizon. More and more cyber attacks took place in the year 2021 targeting not just governmental networks but also corporate networks and individuals apart from their data resident in their computer systems and networks.

---

[1]W., Shanika, and Miklos Zoltan. "15 Biggest Cybersecurity Attacks In 2021 - Privacy Affairs." Privacy Affairs. www.privacyaffairs.com, October 18, 2021. https://www.privacyaffairs.com/cybersecurity-attacks-in-2021/.

[2]*"Domino's Pizza India Data Breach: Name, Address, Other Details Of Over 18 Crore Orders Leaked."* The Indian Express. indianexpress.com, May 25, 2021. https://indianexpress.com/article/technology/tech-news-technology/dominos-data-breach-name-address-other-details-of-over-18-crore-orders-leaked-7328416/.

[3]Dogra, Sarthak. "Data Of Over 700 Million LinkedIn Users Exposed, It Includes Numbers, Addresses And Salary Details." India Today. www.indiatoday.in, June 29, 2021. https://www.indiatoday.in/technology/news/story/linkedin-breach-said-to-expose-data-of-700-million-users-globally-including-number-address-and-salary-details-1820843-2021-06-29.

The figures tell us a scary picture with the world having lost 6 Trillion USD thanks to cybercrimes and cyber security breaches. In the year 2020, the world is supposed to have lost more than 8 Trillion USD. These figures of the growing global cost of cybercrimes and cyber security breaches will continue to keep on proliferating and growing at a massive pace and hence we will have to live with the given ground realities that cyber security breaches and cybercrimes will be our daily companions in our day-to-day digital lives.

Critical Information Infrastructure – The Constant Target For Cyber Criminals

The year 2021 was also the year of increasing attacks on Critical Information Infrastructure across the world. In May 2021, a ransomware attack on Colonial Pipeline halted plant operations for six days in Eastern U.S.[4] The pipeline carries 2.5 million barrels a day - 45% of the East Coast's supply of diesel, petrol and jet fuel[5] hence, the attack led to a fuel crisis and increased prices in the eastern U.S.

Also in June 2021, the Martha's Vineyard and Nantucket Steamship Authority in United States, was victim of a ransomware attack that disrupted ferry services and caused service delays.[6]

On October 14, 2021, closely chasing the cyberattacks targeting the financial, gas, food and transportation sectors, the US. Cybersecurity and Infrastructure Security Agency released Alert AA21-287. The alert turns attention to the fragility of another critical infrastructure sector and warned of "ongoing malicious cyberactivity" targeting water and wastewater facilities. [7]

China in September 2021 issued new regulations to Protect the Critical Information Infrastructure, 'The Regulation for CII Security'. The Regulation delineates the scope and security obligations of the operators of "critical information infrastructure", for purposes of cybersecurity and data security in China.[8]

Consequently, more and more countries are increasingly toying up with new approaches on how to legally safeguard their Critical Information Infrastructure. Different nation-states are also toying up with the idea of coming up with new legal frameworks concerning Critical Information Infrastructure

Legal Approaches to Regulate Cyber Security

[4]Jaskolka, Jason. "Cyberattacks To Critical Infrastructure Threaten Our Safety And Well-being." The Conversation. theconversation.com, October 24, 2021. https://theconversation.com/cyberattacks-to-critical-infrastructure-threaten-our-safety-and-well-being-170191.

[5]Russon, Mary-Ann . "US Fuel Pipeline Hackers 'didn't Mean To Create Problems' - BBC News." BBC News. www.bbc.com, May 10, 2021. https://www.bbc.com/news/business-57050690.

[6]CNN Business, Jordan Valinsky,. "Martha's Vineyard Ferry Disrupted By Ransomware Attack - CNN." CNN. edition.cnn.com, June 2, 2021. https://edition.cnn.com/2021/06/02/business/steamship-authority-ransomware-attack/index.html.

[7]*"Cyberattacks To Critical Infrastructure Threaten Our Safety And Well-being - The Hindu BusinessLine."*, October 25, 2021. https://www.thehindubusinessline.com/info-tech/cyberattacks-to-critical-infrastructure-threaten-our-safety-and-well-being/article37157023.ece.

[8]Amigo L. Xie, Xiaotong Wang, Yibo Wu, Prudence Pang. "Overview Of the New Implementing Rules On Critical Information Infrastructure In China And Key Takeaways | HUB | K&L Gates. October 19, 2021. https://www.klgates.com/Overview-of-the-New-Implementing-Rules-on-Critical-Information-Infrastructure-in-China-and-Key-Takeaways-10-19-2021.

Further, different countries continued their preparations of coming up with their own respective national legal frameworks to deal with cyber security. This became even more apparent as the global vacuum on an agreement concerning cyber security law has pushed nations to start adopting national approaches to deal with the challenges, thrown up by the international paradigm of cyber security.

The Golden Age of Cybercrimes

The year 2021 also saw increasing cybercrimes. The Golden Age of Cybercrimes began with the coming of Covid-19 and continues to consolidate itself in terms of its growth during the various months of the year 2021.

We are now in the golden age of cybercrime. Ransomware attacks have increased dramatically over the past year, with 93% more carried out in the first half of 2021 than the same period last year.[9]

ENISNA, the European Union Agency for Cybersecurity, has released the latest edition of the ENISA Threat Landscape (ETL) report, which analyses cyber-criminal activity between April 2020 and July 2021. It warns of a surge in cyber criminality, much of it driven by the monetisation of ransomware attacks.[10]

Different Cyber Legal Approaches by Different Nation States

The year 2021 also saw the increasing focus of countries on not just coming up with new laws but also amending and revising their laws so as to be more relevant in the context of Covid-19 times. A couple of dedicated laws on cyber crimes have been passed by different countries.

In end 2021, South Sudan has enacted the Cybercrimes and Computer Misuse Provisional Order 2021 aimed to combat cybercrimes.[11]

The Parliament of the Republic of Fiji enacted, on 12 February 2021, the Cybercrime Act which was first introduced by the Government in February 2020. In particular, the Act regulates offences against the confidentiality, integrity, and availability of computer data and computer systems, as well as other computer-related and content-related offences. Furthermore, the Act allows law enforcement officials to seize relevant equipment, issue preservation orders, collect real-time traffic data, and intercept content data, if authorised by a judge and provided that the privacy of third parties is maintained.

In addition, the Act provides for cooperation with foreign governments and cross-border access to stored computer data.[12, 13]

---

[9] https://acurus.com.au/the-golden-age-of-cybercrime/

[10] https://www.zdnet.com/article/ransomware-its-a-golden-era-for-cyber-criminals-and-it-could-get-worse-before-it-gets-better/

[11] https://cipesa.org/2021/12/south-sudans-cybercrimes-and-computer-misuse-order-2021-stifles-citizens-rights/

[12] Cybercrime Act 2021 (Act No. 3 Of 2021). Retrieved at: https://www.laws.gov.fj/LawsAsMade/GetFile/1110

[13] *"Fiji: Parliament Enacts Cybercrime Act 2021."* DataGuidance. www.dataguidance.com, February 19, 2021. https://www.dataguidance.com/news/fiji-parliament-enacts-cybercrime-act-2021.

Through these laws, the nation-states were increasingly focussing on strengthening the hands of nation-states to fight the various challenges of Covid-19 and cyberspace issues.

- **Relevance of Budapest Convention on Cybercrime**

The year 2021 further saw the perpetuation of the status quo pertaining to the legal vacuum at the international level on cyberspace issues. The year 2021 continued to see lack of effective international legal frameworks on how to regulate cybercrimes and cyber security breaches. The Budapest Convention subscribed by more than one-third of nations across the world provides an example for a successful working treaty of cybercrime. However, two-third of nations have not been subscribed to the Budapest Convention.

There are talks of a new convention on the use of ICT for criminal purposes on the horizon. Most stakeholders recognize the vacuum of international agreements on legal frameworks at the international level to regulate cybercrimes and cyber security breaches. Nation states are now increasingly becoming more open to toying up with new approaches on how more effective strategies can be built to tackle the growing challenges of cybercrimes and cyber security breaches.

- **Pegasus Controversy**

The year 2021 was also the year of the Pegasus. Pegasus is a spyware that has been created by the NSO group for the purposes of assisting sovereign governments to surveil and intercept communications using digital networks.

The use of Pegasus software for illegally intercepting and monitoring activities of various stakeholders came to the forefront in a global disclosure made by the groups of publications and newspapers. The widespread use of Pegasus led to an immediate outcry and consequently, different countries started coming up with their own approaches on how to deal with the ramifications of Pegasus.

France launched its investigations in the Pegasus matter. The Pegasus issue was challenged as being violative of peoples' fundamental rights in various Public Interest Litigations (PILs) before the Supreme Court of India. The Supreme Court of India by the landmark judgment upheld the right to privacy and directed the investigation of the use ofPegasus by means of Committee consisting of Court-appointed experts.

The said Pegasus software controversy once again brought to the forefront the need for more checks and balances upon the right to surveillance and the need for more judicial review. However, the growing emerging thought process amongst the nation-states has been that interception and monitoring continue to be important tools for governance for nation-states.

- **Increasing Covid-19 Laws and Regulations**

The year 2021 saw an increase in Covid-19 laws and regulations being passed in different parts of the world. These were in the form of rules, regulations, notifications, directions, and orders issued by various governments and their statutory authorities for the purposes of fighting the menace of Covid-19. However, most of these laws also had the effect of strengthening state power. In my book entitled "New Cyber World Order Post Covid-19", I have argued that by the time the nations are victorious against the current and future waves of

Covid-19 infections, the world will enter into new cyber age where there will be New Cyber World Order awaiting us. More and more states are going to be very powerful in the New Cyber World Order.[14]

Further, cyber security breaches will be the new normal while increasing cybercrimes will be a daily phenomenon. The passing of different laws by nation-states strengthens the proposition that states are increasingly passing laws to enhance and increase state power.

- **Increasing Focus on Data Protection**

The year 2021 saw an increasing focus on data protection.

It was on 3 December 2021 that Zimbabwe enacted the Data Protection Act which also has aspects relating to cybersecurity and cybercrimes. The object of this Act is "to increase data protection in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects".[15]

Kenya had enacted its Data Protection Act even earlier, on 8th November 2019, that applies to data controllers and processors established or resident in or outside Kenya in so far as they process personal data while in Kenya or of data subjects located in Kenya.

As countries across the world were increasingly busy collecting sensitive personal data including health data of individuals to fight the menace of Covid-19 and as vaccinations spread across the world, more and more countries began recognizing the value of data protection and hence, consequently the world saw an increasing focus on data protection in the year 2021.

- **Work From Home Paradigm**

The coming of the pandemic completely changed the paradigm of working. 'Work From Home' became the new normal. Consequently, as different stakeholders were facing teething problems of Work From Home in different parts of the world, nation-states started coming up with their own guidance and advisories on how Work From Home needs to be adopted in the pandemic.

Consequently, different authorities in different parts of the world started issuing rules and regulations as also directions mandating stakeholders to Work From Home and taking appropriate precautions pertaining to the cyber security of their data and Work From Home devices.

We saw that countries also started passing new legal frameworks to promote data protection, cyber security, and thereby contributing to the strengthening of the Work From Home ecosystem.

[14]https://www.amazon.com/CYBER-WORLD-ORDER-POST-COVID-19/dp/B086Y4CRZJ
[15]Media Institute for Southern Africa Zimbabwe (MISA Zimbabwe). "Analysis Of the Data Protection Act | Kubatana." Kubatana. kubatana.net, December 6, 2021. https://kubatana.net/2021/12/06/analysis-of-the-data-protection-act/.

Internet of Things (IoT) & Internet of Behaviour

The year 2021 also saw immense legal developments concerning the Internet of Things (IoT). Internet of Behaviour continued to emerge and consolidate its position. Different countries also began focussing on the cyber security ramifications of the Internet of Things (IoT). For example, the United States of America has come up with the Internet of Things Cybersecurity Improvement Act of 2020. This has been done *"to establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes"*.[16]The act lays down security standards and guidelines for agencies on use and management of Internet of Things devices.

Internet of Things (IoT) and the Internet of Behaviour continue to throw up new legal challenges, which countries across the world are increasingly required to address. The example set forward by California in terms of coming up with the dedicated Internet of Things (IoT) law could be a good starting point for countries to start exploring how they can legally and effectively regulate activities in the Internet of Things (IoT) paradigm.

Intermediary Liability

The issue of intermediary liability continues to be important and significant in the year 2021. With the pandemic in full-blown proportion and with more and more digital users coming on to the internet bandwagon, the world saw the consolidation of the growing power of intermediaries and data repositories. Various instances came forward of arbitrary and unwarranted behaviour on the part of data intermediaries. Consequently, the year 2021 saw the rejuvenating of the growing chorus across the world that intermediaries cannot be left as mute spectators and they have to act as an active participant to prevent the commission of cybercrimes and other illegal activities on their networks.

In September 2021, the High Court of Australia delivered its landmark judgment in the case of *Fairfax Media Publications Pty Ltd v. DylanVoller (S236/2020)*. In the said judgment, the Court held that the administrators and owners of social media pages will be considered publishers of the comments made by third parties on their content. It was further held that it was enough that the owner of the social media page facilitated and encouraged comments thereby insisting on the posting of comments, to find that the owner of social media publishes the comment. Further, the High Court of Australia also held that *"A defendant who does not perform any act of publication personally can still be liable for defamation on the basis of assisting another who performs the act of publication, provided that the defendant assists with a common intention to publish. Consistently with the general principles of the law of torts, assistance can be established by a minor act."*In the said judgment, the High Court of Australia said that intermediaries can be considered as publishers of unwarranted content on their platforms and can be made liable for third-party content.

This development has also to be seen in the context of developments in India, wherein India came up with its new approach on intermediary liability being embodied under the Indian Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. By means of these Rules, India adopted a more stringent approach on intermediary liability thereby specifically exposing intermediaries to criminal liability and also stripping

[16]Congress.gov. "Text - H.R.1668 - 116th Congress (2019-2020): Internet of Things Cybersecurity Improvement Act of 2020." December 4, 2020. https://www.congress.gov/bill/116th-congress/house-bill/1668/text.

them from their statutory legal liability in the event they failed to comply with the said new Rules.

This trend of making intermediaries more answerable appears to be consolidating as different countries are now coming up with new legal approaches on how to force intermediaries to start being more responsible, accountable and transparent in their operations.

Privacy

Privacy continued to be an important concern in the year 2021. The coming of the pandemic also saw more and more people being amenable to foregoing concerns about their privacy protection for the purposes of ensuring that the community and nationsare strong and secure in the fight against Covid-19. However, there has been an increased focus on privacy-related legal developments.

Colorado, in July 2021, joined California and Virginia to become the third US state to pass a comprehensive data privacy legislation, the Colorado Privacy Act (the "CPA").

Under the CPA, consumers may opt out of the processing of their personal data for: (i) targeted advertising; (ii) the sale of personal data; and (iii) profiling in further of decisions that produce legal or similarly significant effects concerning a consumer (provision or denial of financial, lending, housing, insurance, education, criminal justice, employment, healthcare, or essential goods or services). The CPA requires that controllers i.e., businesses provide a "clear and conspicuous" method to exercise the right to opt-out of the sale of personal data or targeted advertising, which must be in the controller's privacy notice as well as in a readily accessible location outside the privacy notice. [17]

Initiatives at Global Level

The year 2021 was also the year when the reports of the various international groups came to be filed. The existing two processes at the United Nations being the United Nations Group of Governmental Experts and the United Nations Open-Ended Working Group, both saw new reports in the year 2021.

The Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security came out in July 2021. The Group underscored the importance of cooperation and assistance in the area of ICT security and capacity-building and their importance to all elements of the Group's mandate. It also identified that increased cooperation alongside more effective assistance and capacity-building in the area of ICT security involving other stakeholders such as the private sector, academia, civil society and the technical community can help States apply the framework for the responsible behaviour of States in their use of ICTs.

The report stated potential areas for future work, which included further sharing and exchanging of views on norms, rules and principles for responsible State behaviour and national and regional practices in norm and Confidence Building Measures (CBMs)

[17] *"The Colorado Privacy Act Signed Into Law."* The National Law Review, Volume XI, Number 197. www.natlawreview.com, July 16, 2021. https://www.natlawreview.com/article/and-now-there-are-three-colorado-privacy-act.

implementation; and on how international law applies to the use of ICTs by States, including by identifying specific topics of international law for further in-depth discussion.[18]

The United Nation Open-Ended Working Group submitted the final report on March 12, 2021. The report identified how the current global health crisis underscored the fundamental benefits of ICTs and the reliance of society upon them.The report also highlighted the continuing increase in incidents involving the malicious use of ICTs by State and non-State actors, including terrorists and criminal groups, calling it 'a disturbing trend' and concluded that any use of ICTs by States in a manner inconsistent with their obligations under the framework, which includes voluntary norms, international law, and CBMs, undermines international peace and security, trust and stability between States, and may increase the likelihood of future conflicts between States. [19]

In addition to technical skills, institution-building and cooperative mechanisms, States concluded that there is a pressing need for building expertise across a range of diplomatic, legal, policy, legislative and regulatory areas. In this context, the importance of developing diplomatic capacities to engage in international and intergovernmental processes was highlighted.[20]

- **Legal Approaches to Regulate Artificial Intelligence**

The year 2021 also saw further developments in the evolution of Artificial Intelligence legal jurisprudence. In the first quarter of 2021, the European Union came up with the draft Artificial Intelligence law for public comments which represented the first major step forward for the purposes of trying to enable regulation of Artificial Intelligence. We are expecting to see far more developments on Artificial Intelligence in the coming times.

- **International Conference on Cyberlaw, Cybercrime & Cybersecurity**

The year 2021 was also significant as the virtual International Conference on Cyberlaw, Cybercrime & Cybersecurity was held from 24th to 26th November, 2021. This Conference not only discussed and deliberated the various aspects of growing evolving legal jurisprudence concerning Cyberlaw, Cybercrime and Cybersecurity but also provided a platform for global thought leaders to interact and discuss emerging trends. The Conference came up with its Outcome Document which is available at https://bit.ly/3m8zhlX, which embodies various recommendations given in various sessions of the Conference. This Conference which is being organized since 2014 every year, has been quietly but efficiently contributing to the evolving legal jurisprudence concerning Cyberlaw, Cybercrime and Cybersecurity.

- **Future of the Internet - Metaverse**

The year 2021 also belonged to the growing awareness and importance of Metaverse. Metaverse started engaging the attention of digital stakeholders as more and more companies

[18]United Nations General Assembly. "Group Of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security." July 14, 2021. https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf.
[19]United Nations General Assembly. "Open-ended Working Group on Developments in the Field Of Information And Telecommunications In the Context Of International Security." March 10, 2021. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.
[20]Ibid.

started announcing dedicated budgets for spending on Metaverse. The city of Seoul became the first city in the world to have a presence on the Metaverse ecosystem. The coming of the Metaverse also brings forward various legal and policy nuances. In my recent Book "The Metaverse Law", I have highlighted some of the key policy and legal challenges that the advent of Metaverse has brought forward. The discussions in 2021 on Metaverse are likely to be further strengthened by more consolidated approaches on further evolution of Metaverse in the coming years.

- **Cyberlaw Jurisprudence Continues to Evolve**

The aforesaid were some of the key and most significant developments in the cyber legal ecosystem which took place in the year 2021. The aforesaid list is by no means exhaustive but is only illustrative of some of the important trends that took place in the year 2021. Clearly, the developments of cyber legal jurisprudence progressed to a new layer of maturity in the year 2021. However, cyber legal jurisprudence is a work in progress. The work done in the year 2021 will be the foundation for the further evolution and development of cyber legal jurisprudence at a global level in the coming times.

To conclude, the year 2021 was the year of the pandemic and in its own manner, the year 2021 contributed by various cyber legal developments to the evolving legal jurisprudence concerning cyberspace and Cyberlaw, Cybercrime and Cybersecurity. We must realize that cyberspace is a great teacher and continues to tell us that each and every week, it is going to bring forward new and distinctive challenges. Hence, there will be a need for digital stakeholders to keep on addressing the constantly evolving paradigms, issues, and challenges thrown up by the cyberspace, the internet and also Cyberlaw 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.