VOL. I/ISSUE I/2021

PAVAN DUGGAL ASSOCIATES

A PAVAN DUGGAL ASSOCIATES INITIATIVE

INTERNATIONAL E-JOURNAL ON CYBERLAW, CYBERCRIME & CYBERSECURITY

WWW.PAVANDUGGALASSOCIATES.COM

EMERGING GLOBAL CYBERLAW TRENDS IN 2021

- **Introduction**

The year 2021 has emerged from the shadows of the year 2020 and it is expected to be an important year in the growth of Cyberlaw jurisprudence at a global level.

This year is likely to see a focus on various thrust areas that are likely to contribute to evolving Cyberlaw jurisprudence.

- **Legal Regulation of Cyber Security**

One of the key Cyberlaw trends globally in the year 2021 will be an increasing focus on legal regulation of cybersecurity. The year 2020 has seen massive cybersecurity breaches. According to a survey, a majority of businesses surveyed needed improvements in their ability to assess financial impact of cyber security breaches between 2019 and 2020 across India. In contrast, only one percent of security leaders felt capable to quantify impact of breaches.[1]
Cybersecurity breachers have started focusing on attacking the Critical Information Infrastructure, apart from the healthcare sector.

Consequently, countries have begun to start legislating on cybersecurity laws to regulate cybersecurity at national levels. The year 2021 is going to see a consolidation of the trends, where countries are going to see an increasing trend towards the enactment of national legislations targeting cybersecurity.

For those countries who already have dedicated cybersecurity laws, they are also likely to work on enhancing the ambit of such laws, apart from coming up with secondary legislations in the form of rules and regulations to support such legislations.

Some countries may continue to go for a softer approach of coming up with national cybersecurity policies and strategies, as compared to dedicated legislations in this regard.

For Countries which have still not made up their minds of coming up with dedicated laws on cybersecurity, the route of national cybersecurity policies and strategies looks more comfortable achievable targets and low hanging fruits.

- **Legally Protecting Critical Information Infrastructure and Healthcare Infrastructure**

The year 2021 is also likely to see a specific focus on coming up with legal frameworks on protection of Critical Information Infrastructure and healthcare infrastructure, given the tremendous attacks that have been targeted during Covid-19 times at the Critical Information Infrastructure and health related infrastructure in different countries. In 2021,

[1] Statista. (n.d.). *India: ability to assess financial impact of cyber security breaches 2020*. [online] Available at: https://www.statista.com/statistics/1201501/india-ability-to-assess-financial-impact-of-cyber-security-breaches/[Accessed 15 Dec. 2021].

the time has come up for countries to start having dedicated Critical Information Infrastructure protection legal frameworks. The year 2021 is likely to see more developments in this regard.

- **Golden Age of Cybercrime and Increasing Cybercrimes**

The year 2021 will see the extension of the growth of cybercrimes.

As per one survey the average cost of a data breach soared to $21,659 per incident during the pandemic, with most incidents ranging from as little as $800 to more than $650,000, according to a new report from Verizon. But 5% of successful attacks cost businesses $1 million or more.[2]

The Golden Age of cybercrimes, which has begun with Covid-19, is going to last for some time. This golden age has demonstrated the inefficacy of existing cybercrime laws to deal with the emerging challenges of cybercrimes. Hence, the year 2021 would see a focus on cybercrime regulation as an important thrust area of growing policies. Countries could potentially be looking up in the direction of having dedicated cybercrime laws.

- **Covid-19 Legal Issues**

The year 2021 is a year where countries are likely to start addressing the distinctive issues thrown up by Covid-19 and the Work From Home paradigm. Covid-19 has propelled increased digitization and has completely changed the Work From Home paradigm. The practical teething problems, that the Work From Home has thrown during Covid-19, is likely to engage the attention of governmental stakeholders as they come up with more enabling legal frameworks to promote the growth and consolidation of Work From Home during Covid-19 and beyond.

- **Increasing Regulation of Artificial Intelligence**

The year 2021 is also likely to see an enhanced trend of legal regulation of Artificial Intelligence. The year is going to build on the efforts made in the year 2020 towards regulating Artificial Intelligence. This year is likely to see the Ad hoc Committee on Artificial Intelligence of the Council of Europe (CAHAI) to consolidate their work on coming up with an international regulatory framework on Artificial Intelligence.

Further, countries are increasingly likely to keep the US as an example in mind and come up with more enabling legal frameworks for regulating Artificial Intelligence in their respective national territorial boundaries.

We are likely to see more developments concerning and acceptance of principles, pertaining to enabling regulation of Artificial Intelligence in the year 2021.

[2] www.cbsnews.com. (n.d.). *Cybercrime is thriving during the pandemic, driven by surge in phishing and ransomware*. [online] Available at: https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/.[Accessed 15 Dec. 2021].

The year 2021 is also likely to see other nations starting coming up with distinctive legislations, even though narrow in nature, which are likely to be focused on different aspects pertaining to regulation of Artificial Intelligence.

- **Regulating IOT Cyber Security**

The year 2021 is further likely to build on the experiences of the world in the year 2020 in terms of regulating cybersecurity in the context of the Internet of Things (IoT). The passing and implementation of the US IoT Cybersecurity Improvement Act, 2020 could potentially act as a catalyst for other countries to come up with similar legislations, to regulate the use of the Internet of Things (IoT) and cybersecurity atnational levels.

- **International Policy Vacuum to Continue**

At the international level, the fragmented policy vacuum pertaining to cyber legal issues is likely to continue to keep on subsisting.

At a time when different countries have already been busy in fighting Covid-19, the chances of these countries to agree to common minimum norms of behavior in cyberspace are not likely to be more bright.

Under normal times during the pre-Covid-19 era, it had taken years and still, no concrete agreement had come forward amongst countries on agreeing to norms of behavior in cyberspace.

Covid-19 provides justifiable opportunities that countries to defer considering the issue of coming to an agreement on international cyber legal norms, including norms concerning the behavior of cyber actors in cyberspace.

- **Legal Frameworks To Promote Use Of Blockchains**

The year 2021 is further likely to see a more enhanced focus on blockchain.

As per one survey the global blockchain market size to grow at a CAGR rate of over 69% between 2019 to 2025.[3]

As blockchains have entered into a new level of maturity and are increasingly being used in different electronic governance initiatives, the year 2021 could see more countries coming up with enabling legal frameworks for promoting the use of blockchains in electronic governance and other applications in the digital ecosystem.

[3] TechJury. (2019). *91+ Blockchain Statistics, Facts, and Trends For 2021*. [online] Available at: https://techjury.net/blog/blockchain-statistics/#gref.[Accessed 15 Dec. 2021].

- **Emergence of New Cyber World Order**

The year 2021 is further likely to see the emergence of different aspects of the New Cyber World Order. In my book "New Cyber World Order Post COVID-19"[4], I have argued how distinct changes are taking place in cyberspace in Covid-19 times, which are likely to result in the New Cyber World Order, by the time the world concludes its fight against Covid-19.

The year 2021 is further likely to see more focus on more enhanced elements of New Cyber World Order emerging. The year 2021 is also likely to see states getting more powerful concerning cyber matters. The same in some cases could have a prejudicial impact upon the enjoyment of digital rights and liberties of netizens.

The year 2021 could also see a migration of users from the superficial net to the darknet.

- **Vaccine Cyber Nationalism**

The year 2021 is also likely to see struggle amongst different nations, in trying to receive the maximum volumes of doses of Covid-19 vaccines. Vaccine cyber nationalism is also likely to increase. Vaccine cyber nationalism refers to a phenomenon where countries will increasingly start using cyberspace and its various facilities for having access to various vaccines, and their related R&D information for the benefit of their populations.

As such, the year 2021 is also likely to see more attacks on the supply chain of vaccines. We are likely to see more cyber attacks on vaccine related data and supply of vaccines, by cybercriminals and state and non-state actors, which will be aimed to disrupt the process of vaccine distribution and dissemination. Hence, the year 2021 is likely to see more countries coming up with enabling legal frameworks to protect the supply chain of vaccine distribution.

Further, with new vaccines continuing to develop across the world, we are likely to see more focus on hacking and unauthorizedly accessing the data pertaining to such vaccines for unauthorized sale or dissemination on the darknet.

- **Consolidation of Cyber Sovereignty**

The year 2021 is further likely to see the consolidation of the trends on cyber sovereignty. More and more countries are increasingly going to put forward expansive definitions of the concept of cyber sovereignty, to enhance the protection of cyber sovereign interests. It is also possible that some countries may want to come up with specific legal frameworks, to enhance the ambit and applicability of cyber sovereign interests.

- **Growing Data Localization Trends**

The year is also likely to see massive data localization trends emerging. These trends could also contribute in the direction of further balkanization of the internet. These trends are

[4] https://www.amazon.in/CYBER-WORLD-ORDER-POST-COVID-19-ebook/dp/B086Q4J76K

built on the fundamental premise that data is the new oil of data economy and that countries need to extensively rely upon data as an element of enhancing the scope and ambit of data sovereignty. More and more countries are likely to discover the benefits of data localization as an effective tool of consolidation of their sovereign interests and are likely to explore options to ensure that data of their citizens does not leave the physical territorial boundaries of those countries.

Russia is further likely to see the consolidation of the implementation of RuNET law which is a legal framework to support building a separate Russian internet to be up and about, in the event Russian internet to the Western World is disconnected.

- **Increasing Interception, Monitoring and Impact on Privacy**

The year 2021 is going to see more and more countries consolidating powers and increasingly relying upon interception and monitoring of data as part of their sovereign functions. This effectively means that this year is likely to see instances where some countries could come up with procedures and processes that are likely to curtain the enjoyment of personal freedoms and digital privacy. Hence, digital privacy is likely to be evaporating more in the year 2021. According to statistics on privacy and security in the USA, just 3% of internet users in the country understand the current laws and regulations in place to protect their data privacy, with 63% either having no idea of or not understanding the regulations altogether.[5]

- **Data Protection Legal Frameworks Under Focus**

Further, the year 2021 is also likely to see more focus on data protection. The General Data Protection Regulations (GDPR) of the European Union is further going to consolidate its position. The GDPR is further likely to encourage member countries to come up with dedicated national laws on data protection.

- **Legal Challenges of Emerging Technologies**

Further, the year 2021 is also likely to see new challenges thrown up by emerging technologies like Quantum Computing which will increasingly bring forward the need for effectively addressing the legal, policy and regulatory issues pertaining to such emerging technologies.

- **Internet Governance Issues Likely To Be Inconclusive**

The internet governance debates at global levels are likely to remain non-conclusive as countries are increasingly using the Internet for covert and overt activities.

[5] legaljobs.io. (n.d.). *18 Chilling Privacy Statistics in 2021*. [online] Available at: https://legaljobs.io/blog/privacy-statistics/.[Accessed 15 Dec. 2021].

- **Increasing Cyber Resilience**

In the year 2021, stakeholders will increasingly have to start adopting a new mindset of cyber resilience, as they struggle to meet the challenges of growing cybercrimes and cybersecurity breaches.

- **Enhancing Cyber Capacity Building**

The year 2021 has once again broughtforward the focus on capacity building. We need to change our mindset concerning cyberspace. There is no denying the fact that cyberspace is now an integral part of our life. Our approaches to cyber resilience and cyber hygiene will have to now substantially change. The year 2021 could start seeing movement in this direction as the year progresses.

The aforesaid are some of the important Cyberlaw trends that one sees on the horizon in the year 2021. Needless to say, one is not a soothsayer and one cannot predict as to what will happen. However, there is no denying the fact that the trends mentioned above should be featuring significantly in the cyberspace landscape in the year 2021.

All said and done, Covid-19 and related developments will have a direct significant impact upon cyberspace as also on Cyberlaw in the year 2021. It will be interesting to see how Cyberlaw jurisprudence evolves in the year 2021.

- **Bibliography**

1) Statista. (n.d.). *India: ability to assess financial impact of cyber security breaches 2020*. [online] Available at: https://www.statista.com/statistics/1201501/india-ability-to-assess-financial-impact-of-cyber-security-breaches/
2) www.cbsnews.com. (n.d.). *Cybercrime is thriving during the pandemic, driven by surge in phishing and ransomware*. [online] Available at: https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/.
3) TechJury. (2019). *91+ Blockchain Statistics, Facts, and Trends For 2021*. [online] Available at: https://techjury.net/blog/blockchain-statistics/#gref.
4) New Cyber World Order [online] Available at: https://www.amazon.in/CYBER-WORLD-ORDER-POST-COVID-19-ebook/dp/B086Q4J76K
5) legaljobs.io. (n.d.). *18 Chilling Privacy Statistics in 2021*. [online] Available at: https://legaljobs.io/blog/privacy-statistics/.