TOP CYBERLAW TRENDS - 2018

BY

Dr. Pavan Duggal
Advocate, Supreme Court of India
President, Cyberlaws.Net
Head, Pavan Duggal Associates, Advocates
Chairman, International Commission on Cyber Security Law

The year 2018 has been a year of tremendous significance that saw massive developments in the Cyberlaw jurisprudence.

We now look at some of the important Cyberlaw events and trends that took place and marked the colour of cyberspace canvas in 2018.

One of the biggest and most important Cyberlaw trends in the year 2018 was the consolidation of cyber security law as an emerging area of Cyberlaw jurisprudence. More and more countries began waking upto the significance of regulating cyber security. Traditionally, Governments and countries were more concerned with having in place enabling legal frameworks for promoting electronic commerce and electronic governance. Information Security was significant but was not given the prime importance from a legislative drafting standpoint. However, the ball started rolling with China enacting its national cyber security law which came into effect from 1st June, 2017. The effect of the Chinese law and the significance of the same began to dawn upon various nations as different countries started their exercises for drafting and passing various cyber security laws in different jurisdictions of the world.

Earlier, in February 2018, Singapore passed its cyber security law which adopted a different approach as compared to the approach adopted by China. The Singapore approach was more holistic, balanced and aimed at development and protection of Singaporean cyber security interests. Soon thereafter, we saw Egypt coming up with its own cyber security law. The year also saw Vietnam passing its cyber security law, which have large number of draconian provisions. These provisions were extensively protested by various corporate players. However, at the time of writing, the said legislation is expected to be implemented in the current form, though, some timeframe is sought to be given to private companies to comply with the same. Various other countries had in the year 2018 also started work, additional or otherwise, on their national cyber security laws and legal approaches. These include countries like Zimbabwe, Australia, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Thailand to name a few.

The year 2018 saw the strengthening of the trend that cyber security is going to be a matter of immense national priority and critical concern for all stakeholders and increasingly would become subject of new distinctive, diverse and complex legislations governing cyber security in various jurisdictions across the world. It is in this context it needs to be noted that different countries have started adopted different legal approaches on cyber security. With the result, number of cyber security laws passed in different jurisdictions, have not presented homogenized approach but has sought to represent diverse thrust areas in different directions. Protection of National security has been an integral part of cyber security legislations. Some countries have, however, gone forward in the direction of stating that the cyber security is part of their national security and hence have sought to see cyber security legislation from the prism and eyes of national security.

To that extent, the various cyber security laws in different countries represent unfolding of the classical story of 5 blind men, trying to describe an elephant. Diverse approaches to cyber security would not ultimately be the best way forward. Hence, there is a need for identifying the commonalities in cyber security law. Aiming to collate the said commonalities in the legal principles governing cyber security, the International Commission on Cyber Security Law is doing its distinctive work of comparative analysis of various cyber security laws. The Commission is in the process of coming up with various legal principles governing cyber security laws, which could then be used by different nations of the world for the purposes of enabling them to come up with their own distinctive national cyber security legislations.

The year 2018 has provided the right thrust to cyber security jurisprudence. It is expected that the said jurisprudence is likely to be substantially strengthened and consolidated in the coming times.

The year 2018 also saw a distinctive new approach to meeting with the challenges raised by encryption technologies for law enforcement agencies. In the second week of December, 2018, Australia passed its national anti-encryption law. The said law has mandated Government and industry players to provide access to the governmental investigative agencies of the encrypted information on their computer platforms. The law has also sought to mandate the industry players to create backdoors in the encryption technologies and work towards the disabling of such security features so as to enable the law enforcement agencies to have access to the said information.

The objectives of the said law are clearly defined to target organized crime and terror activities in cyberspace and the increasing misuse of encryption technologies by cyber criminals and cyber terrorists. However, the said law has also drawn immense criticism from various stakeholders who have highlighted the technological incapability of coming up with such backdoors without comprising the security of encrypted services and platforms. The said law has once again brought forward the issue of efficaciously dealing with global challenges through national legislations and approaches. The said law is currently in a process of review but clearly represents a distinctive new methodology and approach adopted by countries for the purposes of regulating activities done using encryption.

The year 2018 also saw Vietnam coming up with its national legislation concerning cyber security , which has been resisted by various corporate stakeholders.

The passing of broad wide sweeping provisions in cyber security laws in different parts of the world has brought forward the challenge of how the said laws could be effectively implemented. Having in place paper laws is one issue but effectively implementing them is a different issue altogether.

The year 2018 further saw much thrust and focus on the evolving concept of cyber sovereignty. Cyber sovereignty as a concept has evolved couple of years back where countries have been asserting their sovereignty in cyberspace. However, the length and breadth of cyber sovereignty as a concept is a matter of immense discussion and debate. Countries are increasingly seeking to present a very broad definition and ambit for their cyber sovereignty as a means for trying to get a land grab of large chunk of sovereign interests in cyberspace. The year 2018 saw immense discussions and debate on the limitations on cyber security.

Cybersecurity dominated numerous important discussions amongst various stakeholders in the year 2018.

There were numerous other trends that occurred on the landscape in 2018. I would be analyzing them in the next article of mine.

The author Dr. Pavan Duggal, Advocate of Supreme Court of India, is an internationally renowned expert authority on Cyberlaw and Cybersecurity law. 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.