CYBERLAW GLOBAL TRENDS IN 2022

BY

DR. PAVAN DUGGAL
ADVOCATE, SUPREME COURT OF INDIA
PRESIDENT, CYBERLAWS.NET
HONORARY CHANCELLOR, CYBERLAW UNIVERSITY

Global Cyber law trends in 2022 is an interesting subject, which is generating a lot of interest as also discussion and debate. This is so because the cyberspace is constantly evolving and new technologies are beginning to throw up new distinctive challenges.

We need to appreciate that I am not an astrologer who can make predictions, but on the basis of what's appearing on the horizon, it is very clear that there are certain important global cyber law trends that are becoming very significant in the year 2022. Let's examine some of these important trends:

Cybersecurity

2022 is going to see a massive focus on cybersecurity. Clearly, cybersecurity has become the de facto first point of concern for all stakeholders in the digital ecosystem and this particular position is going to be further consolidated and strengthened in the year 2022. We are also going to be seeing the continuation of the current status quo at the international level as far lack of cybersecurity law is concerned. At the international level, there is no one international law on cybersecurity. There is not even one international cyber law in place. This is not surprising because state actors are doing both covert and overt activities and no state player wants to have a naming and shaming process at the global level.

But having said that, we are likely to see far more movement at the national levels on cybersecurity regulations. This becomes imperative because cybersecurity breaches will continue to keep on growing with the passage of time. It has been estimated that by the end of 2021, the world has lost more than $ 6 trillion, thanks to cyber security breaches and this figure is constantly growing.

So, in order to deal with this constant big challenge of cybersecurity breaches, different countries are likely to start coming up with their own distinctive national laws on cybersecurity.

The year 2022 should see the consolidation of this trend. Some of the early movers who have worked up and come up with dedicated laws on national cyber security include China, Vietnam, Singapore and Australia. The year 2022 is likely to see more nations coming up with their own distinctive national laws on cybersecurity. This assumes more significance because of the tremendous number of cyber-attacks that are taking place.

In fact, the year 2022 will see the multiplying of the cyberattacks. Today, cyber-attacks are being engaged in by both state and non-state actors and there are immense number of legal policy and regulatory issues pertaining to cyber-attacks.

Tackling a cyber-attack becomes a distinctive problem. A cyberattack can be originated from one part of the world and targeted at computer systems and communication devices in another country in another part of the world. So, attribution of the cyberattacks becomes a massive concern and this concern will continue to keep on bothering the national and international policymakers in the year 2022.

Ransomware Attacks

Ransomware attacks will continue to keep on increasing. Every 11 seconds, one company, anywhere in the world becomes a victim of a Ransomware Attack and as time passes by in the year 2022 this position is likely to get more worse. Hence, it is expected that nation-state actors are likely to come up with cyber legal frameworks so as to deal with the distinctive challenges of Ransomware.

Cybersecurity Reporting

Further beefing up the national cybersecurity reporting mechanisms is the need of the hour. Various countries have already come up with provisions mandating stakeholders to report cybersecurity breaches. This particular trend is further expected to be consolidating in the year 2022.

Cybercrime

Further the year 2022, is likely to further see the consolidation of the Golden Age of Cybercrime. Cybercrime will continue to keep on increasing and coming up with new manifestations and avatars in the year 2022. Hence, countries across the world are likely to be pushed in the direction of not just revisiting their cybercrime laws at the national level but also to make them more effective and efficacious in these constantly changing cybercrime paradigms. Currently, the economic loss that the world is facing a result of cybercrime and cybersecurity breaches is phenomenal and these particular loss figures will continue to keep on increasing. Hence, more nation-states in the year 2022 are likely to come up with new mechanisms so as to minimise the potential losses caused by cybercrimes to the cyber data economy as a whole.

Artificial Intelligence

The year 2022, is also likely to see a massive push as far as evolution of legal jurisprudence concerning Artificial Intelligence is concerned. Already in the year 2021, we've seen European Union coming up with the Draft Artificial Intelligence, law, which is currently being discussed. This potential draft could become the basis for the further evolution of cyber legal jurisprudence concerning artificial intelligence in the year 2022. Further, different countries are also likely to work on legal principles of artificial intelligence in the year 2022.

Metaverse

We have also seen the emergence of Metaverse in a significant manner in the year 2021. The year 2022 is further likely to see a proliferation, growth and more consolidation of Metaverse as a paradigm. As Metaverse continues to start getting increasingly real, stakeholders across the world will increasingly, in the year 2022, be asked to address the legal policy and regulatory issues pertaining to Metaverse at large, We are likely to see some legal developments on Metaverse law jurisprudence in the year 2022.

Blockchain Technology

Blockchain as a technology, will continue to keep on evolving at a very rapid pace in the year 2022. More modern nation-states are likely to be pushed in the direction of coming up with enabling legal frameworks and provisions concerning Blockchain and the crypto ecosystem. Consequently, a number of nations are likely to come up with legal frameworks to deal with crypto assets and cryptocurrencies. There is a huge debate globally as to whether legal sanction needs to be given to cryptocurrencies but different countries are already taking their own distinctive approaches in this regard. The year 2022 should see more evolution of blockchain law or related legal jurisprudence.

Internet Jurisdiction

Internet jurisdiction is a major issue primarily because while Internet has made geography history. The reality is that it's very difficult to get information pertaining to the attribution of a particular cyber-attack, to particular cyber-actor across boundaries. We've also seen that the mutual legal assistance treaties (MLATs) have not been particularly been very successful as they take a lot of time, effort and energy, and are often not very effective. So clearly the legal and policy issues pertaining to cyber-attacks will continue to be becoming more and more significant and will have to be appropriately addressed at the national level by nation states in the year 2022.

Internet of Things and Internet of Behaviour

We are also likely to see a massive focus on cybersecurity protection in the context of Internet of things and Internet of Behaviour. IoT is the paradigms by means of which not just mobiles and computers, but even smart devices are getting connected to the Internet and these devices are constantly generating data. There has not much been much international unanimity of the minimum standards of cybersecurity. That's the reason why increasingly, it's becoming so easy for any stakeholder to breach the cybersecurity of an IoT device. The year 2022 is likely to see a trend where more countries are likely to work in the direction of coming up with legal frameworks for promoting cybersecurity in the context of IoT.

The previous precedents in the form of the California IoT law and the US Federal IoT Cybersecurity Improvement Act, 2020 could potentially become good precursors and examples for how nation states could potentially be coming up their own national laws on IoT cybersecurity.

Darknet

The year 2022 is also likely to see further growth of Darknet as a paradigm. Consequently, the legal policy and regulatory issues pertaining to darknet will have to be appropriately addressed. As more and more stakeholders are moving onto the darknet, sovereign governments can no longer just close their eyes to the growing importance of Darknet and therefore there needs to be an appropriate, enabling, new legal frameworks so as to regulate some aspects of activities done on the Darknet.

New Cyber World Order Post Covid-19

Clearly, the year 2022, is also going to be near a point where the world will be pushing towards a new cyber age. I have written a book called "New Cyber World Order Post Covid-19". In the said book, I have argued that by the time nations are victorious against the current and subsequent wave of Covid-19 infections, the world will enter into new cyber age where a new cyber world order will be awaiting us. Clearly in this new cyber world order, states are going to become very powerful and further come up with very strong laws to consolidate state power.

In the new cyber world order, there will be increasing cybersecurity breaches, which will be the new default option and there will be increasing cybercrimes as part of our day-to-day lives. There could also be a propensity of nation-states to interfere in the enjoyment of digital liberties. The year 2022 will potentially be pushing the world in the direction of New Cyber World Order and hence digital stakeholders now need to be prepared as to how to deal with the distinctive challenges of this new cyber age and the New Cyber World Order that Is inherent therein.

Growth of Data Economy

We are also likely to see a massive consolidation and growth of the data economy in the year 2022. Clearly, we are living now in a new age where data is the new oil of the data economy. This data economy will continue to be keep on getting more strengthened in the year 2022. More and more nation-states are likely to come up with strong cyber legal provisions and laws for the purposes of promoting and enabling the further growth of the data economy. The data economy is also likely to throw up immense number of legal policy and regulatory issues, which also will have to be appropriately addressed by nation-states as we go forward.

Intermediary Liability

The year 2022, is also going to be an important year as far as the issue of intermediary liability is concerned. This is so because the entire issue of intermediary liability has become a matter of immense concern. With the coming of Covid-19, the intermediaries have become humongous data repositories and have become extremely powerful. Hence, the traditional approach adopted by Section 230 of the US Communications Decency Act, making the service providers completely exempt from all liability for third-party data is a proposition that is increasingly going to be tested, challenges and potentially reviewed at the global level. Ever since the Christchurch Declaration took place we have seen a distinctive trend where more and more countries are inclined towards straddling the intermediaries as data repositories with more

compliance parameters so as to make them more accountable and transparent. I expect this particular trend of demanding more accountability and transparency from intermediaries and data repositories likely to be further strengthened and consolidated in the year 2022.

Norms of Behaviour in Cyberspace

Yet another issue that should assume massive significance in the year 2022 deals with the further evolution of norms of behaviour in cyberspace. This is one very contentious issue that has engaged the attention of the global stakeholders for quite some time. These norms are all the more required because the Internet has transformed the entire world to be one global village and clearly in this global paradigm of cyberspace, there is a distinct need for a global norms of behaviour in cyberspace as far as state as well as non-state actors are concerned.

Quantum Computing

The year 2022 is likely to see more growth in the area of quantum computing. More quantum computers are going to be coming up, thereby propelling us in an age where it becomes easy for the quantum computers to go ahead and break our passwords. Hence, a new approach will have to be evolved, given the unique legal and policy issues quantum computing as a paradigm is beginning to throw up.

Data Protection Laws

The year 2022, is also likely to see an increased activity in the area of data protection. More countries are likely to come up with legal provisions for promoting the cause of data protection.

Work From Home Legalities

Clearly, the pandemic has brought forward the work from home era. The year 2022 is likely to see more maturity in further adoption and growth of work from home. Countries are further likely to come up with new legal provisions and frameworks so as to legally enable work from home so that the entire cause of the global data economy can be appropriately strengthened in the coming times.

Cyber Sovereignty

The year 2022, is also going to be a very important year as far as growth of cyber sovereignty is a concept is concerned. Countries are increasingly concerned that their sovereignty extends not just to their own territorial boundaries, but also to cyberspace. More countries are likely to come up with distinctive national laws so as to further expand the scope of their cyber sovereignty as also for the purposes of addressing the sovereignty, security and integrity of the respective nation-states, both in the physical world and in cyberspace. The year 2022 could also see nation-states coming up with their own distinctive legal provisions which could have an impact upon further enhancing and enlarging the concept of cyber sovereignty of the relevant nation-states in the coming times.

Those are some of the more important cyber law trends that I see at a global horizon in the year 2022. Clearly, the list is not exhaustive. It's only an illustrative list. But, one thing is very clear. The year 2022 is going to build on the massive developments in cyber legal jurisprudence that took place globally in the year 2021. The year 2022 promises to see a lot of action as far as emerging cyber legal jurisprudence is concerned. The advent of new emerging technologies will further be complicating the entire scenario. The year 2022, is also likely to witness an era, where digital stakeholders and policymakers would increasingly be called upon to address a variety of complicated legalities, pertaining to current and emerging technologies that are having a distinctive impact upon activities in cyberspace. All said and done, the year 2022 promises to be an exciting year as far as the further growth and evolution of global cyber legal jurisprudence is concerned.

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.