VOL. I/ISSUE I/2024

A PAVAN DUGGAL ASSOCIATES INITIATIVE

INTERNATIONAL JOURNAL ON CYBERLAW, CYBERCRIME & CYBERSECURITY

WWW.PAVANDUGGALASSOCIATES.COM

GLOBAL CYBERLAW TRENDS 2024

IN

DR. PAVAN DUGGAL
ADVOCATE, SUPREME COURT OF INDIA
PRESIDENT, CYBERLAWS.NET
CHAIRMAN, INTERNATIONAL COMMISSION ON CYBER SECURITY LAW

The year 2024 promises to be a very exciting year as far as cyber legal jurisprudence is going to be concerned. This is primarily because of the vast and rapid developments taking place in cyber ecosystem.

Though at the very outset, I need to state that I am neither an astrologer nor a soothsayer and as such I cannot completely predict with absolute curious as to what is going to happen . However, on the basis of what I see on the horizon and on the basis of my work, I believe there are going to be some key important trends of 2024 which will be very relevant for all digital stakeholders.

Let's look at some important Cyberlaw trends of 2024.

The year 2024 is going to be the year of Artificial Intelligence including Generative Artificial Intelligence. Clearly, Artificial Intelligence has been growing at a phenomenal pace but the manner in which Generative AI has changed the ecosystem, effectively means that the arms-race is now on.

Newer and more powerful AI algorithms including Generative AI algorithms are being developed by companies without pausing to think about the legal ramifications for the same. Every company is jumping the gun on developing new AI machine algorithms, with moral safeguards taking a backseat. This lack of regard for the moral safeguards concerns the lawmakers. So as we are bound to see some very aggressive new products and services in the Generative AI ecosystem, the year 2024 is going to be a major year as far as evolution of Artificial Intelligence Law is going to be concerned.

This is so because AI Law is likely to develop at a phenomenal pace in the year 2024. More and more stakeholders would increasingly be looking at how the legal norms and regulation of AI can be effectively chiselled.

A lot of scholars still believe that AI is good enough to be regulated by the existing regulation. But the very nature of Artificial Intelligence itself shows that existing legal frameworks may not be adequate to deal with Artificial Intelligence. AI is a dynamic system which changes as the sands of time pass on. That is the reason why different countries across the world have already started coming up with their own distinctive national laws on Artificial Intelligence.

China has come up with the world's first law on Generative AI and implemented the same on 15th August, 2023. The European Union AI Act has been in the pipeline for some time.

However, the new massive quantum developments in Generative AI effectively means that the time has come for them to have a relook at their proposed legal frameworks.

New York has come up with its own distinctive legal framework pertaining to Artificial Intelligence. The focus of these and more legislations will continue to somehow deal with the bigger challenges that Artificial Intelligence is beginning to throw up.

Hallucination of content by AI is going to be one of the bigger problems and the bigger priority areas for the lawmakers to focus in the year 2024. Similarly to ensure that humans are not discriminated against by the discriminatory approaches and the bias intrinsic in AI algorithms appropriate legal frameworks will have to evolve and specify new provisions and parameters in this regard.

Further, the year 2024 is likely to see massive use of AI for purposes of not just cybersecurity breaches but also for the purpose of committing various cyber-criminal activities. Hence, AI crimes and AI cyber security breaches are going to become increasingly more and more predominant as the year passing by.

This effectively means that there will now increasingly be demand and need felt by stakeholders across the world so as to curb the misuse of AI for cyber breaches or for the purposes of committing cyber-criminal activities or cybercrimes. In this regard, some of the existing national laws on cyber security and on cybercrimes could potentially be invoked, but clearly because of the intrinsic character of Artificial Intelligence, the time has come for the world to come up with new legal frameworks to deal with AI cyber security breaches and AI cybercrimes.

This is going to be one of the most crucial thrust areas as far as growth of cyber legal jurisprudence globally is going to be concerned. Countries are also realising that there is no international legal framework to regulate Artificial Intelligence . Therefore there could even be a push where countries could begin to start emphasising the need for coming up with international legal framework to regulate AI. Law makers are likely to move in the direction of making an AI global equivalence of the Non Proliferation Treaty, in order to keep the proliferation of Artificial Intelligence in check.

Clearly, when one looks at the various ethical frameworks already proposed for AI, a lot of work has been done in this regard, but merely having in place ethical principles and framework for AI may not suffice. At the end of the day, you will require effective and efficient legal frameworks to back up the enforcement of ethical standards and principles in this regard on the ethical ramifications of AI. Legal framework would need to stipulate the right and wrong in the usage of Artificial Intelligence.

No wonder, the growing talk about Responsible AI is getting more and more topical. We could even see some countries pushing the agenda for having in place minimum common denominators or agreed principles which could be agreed by nation states as they come together in the direction of trying to regulate AI at an international level. There is no denying the fact that AI will become the juggernaut of the 21st century. That being so, the chances of AI being used against human interests, human values and human liberties is going to be very high. Hence, the impact of AI on human values is going to be of crucial importance.

Well, Elon Musk has already stated that AI has become an existential threat to mankind. This existential threat is going to continue to keep on growing and developing, with the passage of time. Hence, quick mechanisms to prevent the misuse of AI against human interests will have to be the top most priority for government and various stakeholders as we go forward in the year 2024.

The year 2024 could see legal frameworks for determining the legality of output of Artificial Intelligence as also determining the liability aspects of Artificial Intelligence. Popular media with the likes of cinema, books, short-stories etc. has shown the rising dangers Artificial Intelligence could impose. The misuse of Artificial Intelligence for creating harm and injury is going to be massive in the coming times, which will prove the fears shown by the popular media. Hence, the legal liability principles which will be applicable in the context of harms caused by Artificial Intelligence will basically have to be evolved with the passage of time. The year 2024 could see some important developments taking place in this regard at the level of different countries.

Further, this year is also going to see extensive use of Artificial Intelligence so as to prejudicially impact the free fair level playing field for stakeholders in the digital economy. There are going to be increasingly efforts to misuse AI to promote anti-competitive behaviour and to further go ahead and further expose various consumers to more discrimination and price speculation using AI. This will be one area that will increasingly be engaging the attention of competition regulators globally.

The time has come where in 2024, the competition regulators will increasingly have to come at a very quick pace and start developing the norms of the time so that the misuse of Artificial Intelligence for prejudicially impacting competition issues could be minimised to the best extent possible.

Cyber security of Artificial Intelligence will have to also become a very important thrust area as far as legal regulatory frameworks are going to be concerned. Today, when we don't exactly know what exactly are various building blocks of AI algorithms, the chances are that these building blocks could be manipulated in terms of their cyber security to prejudicially impact the outcome of Artificial Intelligence algorithms and generative capabilities.

Hence, minimum parameters for ensuring the protection and preservation of cyber security in Artificial Intelligence will also increasingly become an important priority and thrust area for countries to start regulating and coming up with norms in this regard.

The year 2024 is also likely to be the year where AI jurisdiction is going to develop into a big paradigm. We already are living in cyberspace where internet has made its mark in making geography, history, Today, the internet jurisdiction issues are going to get far more confounded by the applicability and invocation of Artificial Intelligence across national territorial boundaries so as to cause wrongful loss, harm or injury to stakeholders located in other jurisdictions across the world.

Attribution of acts done by AI will have to be also very important thrust area which will engage the potential attention of lawmakers as we move forward.

The most important element in the year 2024 will be how do countries go ahead and legally define the legality of Artificial Intelligence. Can Artificial Intelligence be given a legal status

in terms of being a legal entity? If so, what are going to be the legal ramifications and consequences arising there from? This is going to be a major issue that will engage the attention of lawmakers across the world.

Clearly, the experience so far has been that lawmakers are by and large shying away from addressing this particular issue, while trying to just address fringe issues. But clearly, legality of Artificial Intelligence is a million dollar question. If answered properly, it could open up new vistas of growth, opportunities and new progress that human civilisation has not yet seen.

The increased use of Artificial Intelligence in different verticals and areas of human endeavours means that the year 2024 could also see the emergence of vertical specific regulations concerning Artificial Intelligence. Hence, specific regulators of specific industries are likely to come up with new guidance and inputs on how AI needs to be enforced and implemented in the context of specific verticals, disciplines and areas of human activities and endeavours.

We are likely to see proliferation of use of Artificial Intelligence in governance ecosystem. Hence, the need for ensuring the impartiality of output of Artificial Intelligence for governance purposes will have to be legally ensured. In this entire ecosystem, the AI companies and AI coders cannot be left far behind. Very quickly the attention of the lawmakers across the world is going to grow and focus on these AI coders and AI service companies. They would increasingly be now facing a new wave of regulation where they are going to be made responsible to some extent regarding the activities or acts, deeds or things which are done by Artificial Intelligence.

Hence, due diligence and appropriate safeguarding that will have to be followed by AI companies and AI service providers will be an important thrust area as far as Cyberlaw jurisprudence in the year 2024 is concerned.

We have discussed some of the broad thrust areas on the manner in which Artificial Intelligence legal jurisprudence is likely to evolve in the year 2024. However, the year 2024 is not just only about Artificial Intelligence Law and legalities, the year 2024 promises to become a very colourful year. This will be the year where we would be seeing an unprecedented rise in cybercrimes and unprecedented growth in global cost of cybercrimes.

As per one estimate, the world has already lost more than 8 Trillion USD to cybercrimes by the end of 2023. The chances of this figure increasing in a dramatic manner in 2024 are very much existing.

With ransomware, Distributed Denial of Service Attacks (DDoS) and malware attacks being rampant, it is only a question of time when their continued economic impact upon the economies of the world is likely to be coming to the attention of the Governments. Hence, the year 2024 would also see a new trend where countries could look at the need for beefing their national cyber legal frameworks in such a manner so as to go ahead and make these laws more relevant, topical and contextual in the context of rise of newly emerging crimes.

Already the Golden Age of Cybercrimes has begun with the coming of Covid-19. We are likely to see more consolidation of Golden Age of Cybercrimes and as cyber criminals become more advanced and more tech savvy, vis-à-vis their approaches, methodologies and processes, the year 2024 is likely to put more pressure on lawmakers so as to beef up their cybercrime laws so as to meet with the growing challenges of cybercrimes and also to make not just their

legal frameworks more deterrent but also effectively provide for mechanisms to promote more cybercrime convictions in the respective countries.

The year 2024 is also likely to see further growth and impetus in cyber security breaches. Cyber security breaches have by and large become the norm of the day and it is only a question of time as to when you are likely to become a victim of cyber security breach.

In this context, it becomes absolutely imperative for countries to start coming up with effective practical and deterrent legal frameworks to deal with the rising challenges of cyber security breaches.

Number of countries have already come up with national laws on cyber security. The chances of the said trend of such national laws increasing and getting more consolidated is likely to increase in the year 2024. We are also likely to see sector specific cyber security legal frameworks and regulations coming in.

Sectors like Critical Information Infrastructure, Banking and Financial Services & Insurance (BFSI) and Health sectors are particularly likely to see more regulatory frameworks and provisions evolving globally in this context. This is so as existing frameworks are ineffective and are susceptible to cyber attacks.

There will increasingly also have to be new legal models adopted as to how the legal liability for data breach notification provisions need to be effectively calculated. More and more countries have come up with their dedicated legal provisions on data breach notification, which provisions are further likely to get enhanced and more consolidated.

There will have to be increasing pressure on companies to ensure that they comply with the requisite provisions pertaining to cyber security protection as also data breach notification in order to limit their legal liability from exposure to potential civil and criminal consequences.

The focus will have to be on all stakeholders going ahead and adopting a culture of cyber security and legal frameworks and principles can play an important role in persuading stakeholders to ensure compliances with cyber security.

The year 2024 is also likely to be a year where we are going to see some massive growth as far as number of connected devices is concerned. More and more connected devices in the world now means that Internet of Things (IoT) is now getting more mainstream and countries would now increasingly be called upon to come up with new legal frameworks so as to regulate the mounting misuse of Internet of Things (IoT) and Internet of Behaviour.

In this regard, we have already seen number of countries coming up with national legal provisions on Internet of Things (IoT). We believe this kind of trend is likely to be further consolidated and growing in the year 2024.

As technology is moving at a very rapid pace, the year 2024 could also see more focus on countries trying to update their cyber legal frameworks so as to make them more topical, relevant and pertinent in today's changed technological ground realities.

In this context, we could see fragmented developments concerning Cyberlaw jurisprudence at a global level. The year 2024 could also see a new thrust where in different parts of the world,

the focus will be on dealing with the contentious issues of crypto-assets and crypto-currencies as technological paradigms.

The growing maturity of blockchains has ensured that now blockchain is no longer a mirage but is now a concrete reality. However, the legalities pertaining to blockchains will have to be appropriately addressed, depending upon the national priorities of the concerned national governments. In this regard, we could see some diverse developments. There is no uniformity in the approach of countries as they are dealing with crypto ecosystem. Most of the countries are trying to come up with their own customised approaches on the legalities of crypto-assets, bitcoins.

With more focus on startups and with new technologies evolving, the focus of Cyberlaw jurisprudence in the year 2024 is going to be more on flexibility. Jurisprudence will have to be more flexible so as to not just provide for more elastic development in this field but more significantly also to provide adequate flexibility to lawmakers and policymakers in coming up with their own customized approaches on dealing with various legal, policy and regulatory challenges that the technology is beginning to throw up.

In addition, as new technologies are evolving, the impact upon personal spaces, personal privacy and data privacy is increasingly going to be felt. Hence countries are likely to experiment with new legal provisions and frameworks so as to give adequate protection to personal privacy and data privacy of digital users in the constantly changing technological paradigm.

Issues like data protection will continue to be the topical and relevant because of the advent of data economy and with data being the new oil of the data economy, there will be increasing emphasis on stakeholders to ensure compliance with applicable legal frameworks on data protection.

For those countries who don't yet have legal frameworks on data protection, they are likely to see new developments where we could see new legal provisions on data protection in some jurisdictions.

The aforesaid are some of the more important developments in Cyberlaw jurisprudence which are likely to take place in the year 2024. We need to appreciate that the list made above is neither complete nor comprehensive but only represents some of the key important areas and developments that I expect the world is likely to see in Cyberlaw jurisprudence in the year 2024. It is very much possible that we can see far more other new developments pertaining to new technological paradigms in the year 2024.

The year 2024 promises to be the year of action and a lot of action is likely to be visible in the cyber legal jurisprudential trends. Hence, this will be one key thrust area that will be of importance and interest for Cyberlaw practitioners and digital stakeholders as they navigate their ways through the choppy waters of digital and cyberspace and the uneven bounces of newly emerging technologies.

It will be great to look at some emerging developments on Cyberlaw jurisprudence in the year 2024, to learn from them and hopefully these developments of the year 2024 could become as building blocks for the purposes of further evolving the future development of Cyberlaw as a discipline, globally and regionally and also in different nations across the world.

The author Dr Pavan Duggal is internationally renowned expert and authority on Cyberlaw, Cyber Security Law, Artificial Intelligence and emerging technologies. He is the Chairman of the International Commission on Cyber Security Law and has been acknowledged as one of the top four cyber lawyers of the world. He can be reached at his email addresses pavan@pavanduggal.com and pavanduggal@yahoo.com. More about Dr. Pavan Duggal is available at www.pavanduggal.com.