IMPORTANT GLOBAL CYBERLAW TRENDS 2017

BY

PAVAN DUGGAL
ADVOCATE, SUPREME COURT OF INDIA
PRESIDENT, CYBERLAWS.NET
HEAD, PAVAN DUGGAL ASSOCIATES, ADVOCATES

The year 2017 promises to be a year of tremendous developments as far as Cyberlaw jurisprudence is concerned.

The year 2017 is likely to build upon the foundations of Cyberlaw jurisprudence which has been placed at a strengthened position in the preceding years especially in the year 2016. It is hard to crystal gaze and predict specifically. However, on the basis of the information available, some broad trends of Cyberlaw jurisprudence can be detected on the horizon.

1. CYBER SECURITY LEGAL APPROACHES

The first biggest trend on Cyberlaw jurisprudence that the year 2017 is likely to see emerging cyber security legislative instruments and legislative approaches. Cyber security over the last few years has ceased to become a merely technical issue. On the other hand, it is becoming a very critical Cyberlaw, policy as well as regulatory issue. Different countries have already started coming up with different legislations and policies concerning cyber security. The year 2017 is likely to see more countries coming up with detailed legislative frameworks as also national policies impacting cyber security. The difference of approaches, which the specific countries will make, will be dependent on the peculiar challenges that they face from time to time. Some countries are likely to introduce significant cyber security laws while other countries are expected to go through soft legislations route, by coming up with national policies and appropriate guidelines to govern cyber security ecosystem and the roles, duties and responsibilities of respective stakeholders therein.

2. BILATERAL CYBER SECURITY AGREEMENTS

Another important trend in Cyberlaw jurisprudence that is likely to evolve will be increased adoption and execution of cyber security bilateral cooperation agreements and arrangements. Countries across the world have recognized that there is lack of an international Cyberlaw on cyber security. Countries further recognized that cyber security is a global paradigm and that it would require global approaches to be effectively dealt with. However, countries are also appreciating that it will take some time for international Cyberlaw frameworks to be put in place. Hence, more and more countries are likely to go in for bilateral cyber security arrangements and cooperation agreements as also anti-hacking agreements with other countries. These arrangements and bilateral treaties would aim to strengthen cooperation mechanisms between countries and provide for more sharing of information concerning protecting and preserving cyber security as also information concerning cybercrimes. These bilateral agreements and

arrangements are further going to contribute to the crystallization of key international principles impacting Cyberlaw and cyber security which countries could agree upon, thereby contributing to the development of international jurisprudence concerning cyber security law.

3. INTERNATIONAL COMMONLY ACCEPTED PRINCIPLES AND DENOMINATORS IMPACTING CYBERLAW

The year 2017 is further likely to see more discussions and debate upon coming up with international legal framework impacting cyberspace. The absence of an international cyberlaw has necessitated that countries look at common legal principles impacting the regulation of cyber issues at a global level.

The year 2017 is likely to see further discussion moving in the direction of distilling the international commonly accepted principles and denominators impacting Cyberlaw which could then be part of an international treaty. The Author has already mooted the idea of the need for having in place an International Convention on Cyberlaw & Cybersecurity in 2015 itself. As the world begins to see more global threats emerging to the security and stability of the Internet, there is likely to be more calls for coming up with common minimum denominators and principles of international law which could then contribute in the direction of an International Convention on Cyberlaw & Cybersecurity.

4. LEGISLATIVE APPROACHES GOVERNING EMERGING CYBERCRIME

Another important trend that the year 2017 is likely to see is the increasing attempts at legislative approaches aimed at regulating emerging kinds of cybercrimes. Cybercrimes are continuing to proliferate with each passing day. Newly emerging kinds of cybercrimes like ransomware have already impacted industries worldwide. The advent of the Darknet and cyber criminals activities originating therefrom provide further legal headaches and challenges for law enforcement agencies across the world. In this context, the year 2017 is likely to see more movements in the direction of strengthening national legislative approaches and legal frameworks regulating cybercrimes. Meanwhile, the year 2017 is likely to see far more calls for closer cooperation at the international level concerning cybercrime information sharing and strategies for getting effective prosecutions in cybercrime matters.

5. DARKNET JURISPRUDENCE

The year 2017 is further likely to see more work happening on developing the legal jurisprudence concerning the regulation of cyber criminal and illegal activities done on the Darknet. Hence, there is a need to work on attribution related principles concerning cyber criminal activity on the Darknet.

6. PRINCIPLES IMPACTING ATTRIBUTION OF CYBER CRIMINAL ACTIVITIES IN CYBERSPACE

Another important significant Cyberlaw jurisprudence trend that is likely to emerge in the year 2017 would relate to crystallizing and developing principles impacting attribution of cyber

criminal activities in cyberspace at international level. Internet has made geography history but the same boundary-less medium is sought to be regulated by national legislations. Consequently, internet jurisdiction continues to be a big legal problem.

7. INTERNET JURISDICTION

More work needs to be done on tackling the legal challenges raised by the Internet jurisdiction in the year 2017. Cyber criminals often hide behind the anonymity on the Internet as also the complex challenges raised by Internet jurisdiction to escape exposure to potential prosecution. Globally, the discussion is likely to be distilled further in the direction of evolving strong and sound legal principles impacting attribution of criminal activities on the Internet.

8. INTERNET OF THINGS LEGALITIES

The year 2017 is further likely to see more work happening to develop the legal principles governing Internet of things and transactions made thereon. With 24.8 Billion[1] number of devices expected to get connected with Internet of things by 2017, cyber security and protection of privacy become important vectors on which legal frameworks need to be developed. As the year 2017 witnesses more adoption and usage of Internet of things, it is also likely to see more work on the legalities and legal principles governing Internet of things, more so in the context of cyber security, personal and data privacy as also data protection issues connected therewith.

9. DATA PROTECTION IN A UBIQUITOUSLY CONNECTED INTERNET

The year 2017 is further likely to see more discussion and debate on how to ensure data protection in a ubiquitously connected Internet. Countries may look at different approaches prevailing in the global scenario to modify and remodel existing data protection strategies aimed at protecting data effectively and efficaciously.

10. CONSUMER PROTECTION ISSUES

As more and more consumers join the digital bandwagon at the global level, we are likely to see further jurisprudence evolving concerning consumer protection issues in cyberspace. Consumer protection issues are already marked as important issues in some jurisdictions while in other jurisdictions, consumer protection is virtually non-existent. The year 2017 is likely to see further development of jurisprudence impacting consumer protection in the year 2017.

11. BLOCKCHAIN LEGALITIES

The year 2017 is further likely to see more work being done on the legalities pertaining to blockchains as a transformative technology. With increased adoption of blockchains in banking, financial and other sectors, there is a need for more work to evolve jurisprudence concerning blockchains at a global level. The further adoption and strengthening of usage of crypto currencies across the world further means that work on the legal challenges raised by crypto

[1] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

currencies need to be done in 2017 so as to enable countries to have common minimum platform of regulating activities done using crypto currencies.

12. SOCIAL MEDIA JURISPRUDENCE

Social media will continue to rise in 2017. New social media platforms are increasingly engaging the attention of the netizen community. The legalities concerning social media jurisprudence require more discussions and debate. There is an urgent need to protect women and children on social media from unwarranted exposures and influences and Cyberlaw needs to play a significant role therein

13. CYBER RADICALIZATION AND CYBER TERRORISM

As cyber radicalization and cyber terrorism continue to grow unabated, the year 2017 is likely to see more focus on coming up with national and international frameworks to effectively regulate the same. Counter narratives to deal with cyber radicalization, would require enabling legal support from legal frameworks all over the world. Cyber terrorism jurisprudence would need to be expanded in 2017 to cover the emerging new activities being engaged in by cyber terrorists all over the world.

14. REGULATION OF INTERMEDIARIES AS DATA REPOSITORIES

The year 2017 is likely to see more focus on the regulation of increased role of intermediaries and service providers as data repositories , with increasing compliance and due diligence requirements. Countries across the world are increasingly likely to examine the important complex role played by the intermediaries in the cyber ecosystem and put more responsibility on such data repositories concerning cyber security as also protection of third party data.

15. DATA PROTECTION AND PRIVACY

The year 2017 is further likely to see the focus on protecting and preserving data as also personal privacy. In that context, the year 2017 is likely to see increased discussion and debate on how to protect and preserve data and personal privacy in accessing consumer data.

16. ENCRYPTION BALANCING

Since encryption is a very important subject, the year 2017 is likely to see further calls for need to develop legal principles in such a manner which can help create golden balance between protection of privacy using encryption and the intrinsic rights of the sovereign states to have access to backdoors.

17. INDIVIDUAL RIGHTS VERSUS CYBER SOVEREIGNTY

The year 2017 is further likely to see a conflict emerging between protection and preservation of individual rights on the Internet and increasingly bigger ambit of cyber sovereignty of sovereign nations. As freedom of speech and protection of fundamental rights on the Internet engage the centre-stage attention in different jurisdiction, Cyberlaw jurisprudence is likely to be called upon

to develop robust effective and efficacious principle which can help balance both the competing demands from different stakeholders in a delicate manner.

18. NORMS OF BEHAVIOUR IN CYBERSPACE

The year 2017 is further likely to see more discussions on the applicability of international law to cyber warfare issues. Discussions around rules and norms of behavior in the cyberspace expected from all stakeholders in the cyber ecosystem will increasingly engage the attention of the relevant stakeholders.

The aforesaid are some of the important trends in Cyberlaw jurisprudence that one can detect emerging in the horizon. Needless to say, I am not a Soothsayer and it is not possible to predict comprehensively. However, on the basis of the developments that have taken place in the year 2016 and earlier years, it is expected that the aforesaid issues will increasingly become more significant in terms of their importance and would further help in contributing to the evolving Cyberlaw jurisprudence at global, regional and national levels.

It will be interesting to see how the jurisprudence concerning Cyberlaw issues, aspects and subjects will actually evolve in a robust and efficient manner in the year 2017.

The author Pavan Duggal, Advocate, Supreme Court of India, is Asia's & India's leading expert and authority on Cyberlaw, Cyber Security Law & Mobile Law and has been acknowledged as one of the top four cyber-lawyers in the world. He can be contacted at his email addresses pavan@pavanduggal.com and pavanduggal@yahoo.com. More about the Author is available at www.pavanduggal.com and http://www.linkedin.com/in/pavanduggal.