Pavan Duggal:

Cyber Terrorism And Cyber Law - Duties Of Service Providers

Abstract:

The year 2017 has dawned in a new era. This is an era where cyber terrorism and cyber extremism are increasingly going to be significant factors in our day-to-day lives. Whether we like it or not, today social media platforms are infiltrated with cyber terrorists and cyber extremists. In addition, Cyber radicalization as a phenomenon is constantly on the rise.

Agenda

Author:

Mr. Pavan Dugal:

- Advocate, Supreme Court Of India, President, Cyberlaws.Net, Head, Pavan Duggal Associates
  S-307, LGF, Greater Kailash-1, New Delhi, Delhi 110048
  pavan@pavanduggal.com; pavanduggal@yahoo.com
- Expert and authority on Cyberlaw & Mobile Law; acknowledged as one of the top four Cyber-lawyers in the world. More about the Author is available at www.pavanduggal.com and http://www.linkedin.com/in/pavanduggal

ISSN 1614-1687

Important Cyberlaw Trends Of 2017

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.

Consumer Protection Issues

As more and more consumers join the digital bandwagon at the global level, we are likely to see 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.

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

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

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.

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.

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.

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.

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.

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.

Duties of Service Providers

The rationale behind the emerging trends is crystal clear. Cyber terrorists are increasingly focusing on those areas on the Internet where majority of people are converging and social media platforms are clearly one of them. Consequently, more and more cyber terrorists are infiltrating social media networks. It is common knowledge that cyber terrorists are using social media for outsourcing terrorist designs and approaches as also for disseminating terrorist contents for misleading innocent young minds accessing the Internet.

In this scenario, the entire role of intermediaries and services providers becomes critical. Recently, it has been reported that Twitter as social media network has been sued by a Florida woman Tamara Fields, whose husband Lloyd died in a terrorist attack. The plaintiff has accused Twitter of having knowingly allowed ISIS as a terrorist group, to use the Twitter network to spread propaganda, raise money and attract recruits. Twitter has denied the said charges.

While we await the decision of that case, the important factor that is gaining centre-stage attention is that intermediaries and service providers increasingly have a duty to ensure that their networks are free from dissemination of cyber terrorist content as also data.

Gone are the days where service providers were merely pipe providers. Today, the service providers and intermediaries have undergone metamorphosis into huge data repositories. In today's scenario, service

providers and intermediaries have various obligations, though the said obligations are not being completely complied with.

Going forward, I am of the view that today service providers and intermediaries need to be straddled with some basic duties in the context of cyber terrorist content on their network. I enlist 6 important legal duties for intermediaries and service providers, which become more relevant and topical in today's times:-

a) Service providers have a duty to take care and caution towards ensuring that their networks do not get misused for cyber terrorist and cyber extremism purposes.

b) The service providers have a duty to exercise due diligence while discharging their duties under the law.

c) The service providers further have a duty to ensure the security and stability of their networks and further ensure that their stable, secure networks are not prejudicially impacted by cyber terrorist content, propaganda as also information in any manner.

d) Service providers also have a duty to protect the members/users on their platforms from exposure to undesirable cyber terrorist and cyber extremist data and content.

e) There is a duty for service providers to be sensitive of the sensibilities of users on their networks.

f) Intermediaries have a larger societal responsibility towards ensuring that their networks do not get misused as tools for dissemination and propagation of terrorist content and information as also platforms for enabling cyber terrorists to target their respective targets.

It needs to be noted that most of these duties are already intrinsically known to stakeholders, though they are often not enforced. All the aforesaid duties are those, which appeals to common sense and need to be duly documented in cyber legal frameworks to ensure that service providers mandatorily comply with the same.

Seen from the perspective of service providers, the service providers may not necessarily welcome imposition of any such duties on them. They would take the argument that they already have been straddled with enough other compliance. Further, in the context of the United States, service providers take the plea of exemption from liability as service providers in their capacity under US laws.

The service providers often also argue that the responsibility of fighting cyber terrorism is purely that of the Government and that the Governments cannot outsource their statutory and sovereign functions to be performed by service providers. While that argument may have some merits that still does not mean that intermediaries and service providers can look the other direction, while their networks are being misused for dissemination, propagating or spreading cyber terrorist content and information.

The entire issue pertaining to intermediary liability needs to have a relook, given the fact that the world is now going through a changed scenario. A new chapter needs to be written in the evolving jurisprudence on intermediary liability. Further, countries in different parts of the world increasingly now need to focus on documenting the aforesaid duties of care for intermediaries and service providers to ensure that the said intermediaries do not in any manner, conspire or abet in the commission of any cyber terrorist activities, merely by virtue of them providing their platforms for the dissemination, spread, propagation of cyber terrorist activities, information, data as also propaganda.

We need to quickly realize that cyber terrorism, cyber extremism and cyber radicalization are three sisters which combined together, can have the effect of prejudicially impacting not just the Internet but also societies and nations at large. In such a scenario, Cyberlaw frameworks need to develop quickly to enforce the duties

of intermediaries towards ensuring that their networks are not misused or abused by cyber terrorist activities or cyber extremism forces.

As the world wakes up to a new era, the three sisters of cyber terrorism, cyber extremism and cyber radicalization are beginning to make their prejudicial impact felt. It is high time that Cyberlaw as a jurisprudence evolves in the direction of ensuring the protection and preservation of Internet as a network of network and also for implementing the manifestation of peoples' expectations that social media networks should not be allowed to be misused for cyber terrorism, cyber extremism and cyber radicalization purposes.