The Ascendant cycle of Cyber Crimes: An ordeal for the present Legal framework

Dr. Rahul Vyas
Assistant Professor, Pacific School of Law, Paher University, Udaipur

Abstract

The ubiquitous expansion of the world wide web (www) and as predicted by Gordon Earle Moore – The Moore's law technology has evidenced an exponential advancement globally leading to the escalation of innovative types of white collar crimes, in particular the web based. Also the web space is expanding exponentially with an unregulated upswing in web based business transactions and what not. Novel business formats and models are emerging at a drop of a hat and yet more are being explored and designed. From AirBnB, Amazon, Myntra to Zomato an endless list of website are witnessing a stupendous growth in E-biz, but always lurking in the digital world are dark net pilferers - the hackers, the phishers, site squatters and a host of other dark net denizens. These crimes are in the virtual world and as there are no physical boundaries that constrain the world wide web they have the potential to distress any person across the globe including even Hillary Clinton.

Today cyber crime has turned into a career choice and the demographic of a representative cyber criminal is shifting swiftly from a geeky nerd to a conventional mafia gangster generally linked to money laundering, drug-trafficking and extortion etc.

The present paper is a conceptual paper which endeavors to explain the challenges that confront the legal governance in the country.

Keywords: White Collar Crime, IT Act 2000, Cyber Laws

Introduction

The tectonic shifts in Technology and advent of Algo's, AI, ML and Robotics have made a sea of difference in the strategy for business. E-commerce is being used for sale and purchase of several products and services using diverse portals and website.

The latest assault by the WannaCry ransomware as reported by The Telegraph "appears to have used a flaw in Microsoft's software, discovered

by the National Security Agency and leaked by hackers, to spread rapidly across networks locking away files." In March 2017 a research by Tele Sign and RSA, has revealed that only 11% of US companies responded that they have not experienced any fraudulent occurrence on their e-commerce sites in the past year.

In December 2016 research by Adroit Digital said that 68% of US internet users reported the chief way they would counter a security breach at a website or brand would be to stop using the same as against just 7% who said they were not bothered by it.

Legal Enforcement and Cyber Crimes

The IT Act, 2000 in its present avatar is ill equipped to take on the evolving cyber crimes. Which comprise of either A) where the Computing Machine itself is the Target i.e. using a PC to launch a cyber assault on other PCs and machines? Like hacking and the Wannacry style Virus attacks. Or B) The use of the computing Machine as a weapon - Trolling, Fake News, IPR infringements, online frauds etc.

The conventional laws depend heavily on documents but with the advent of web based commerce and Data it has become imperative on the part of our country's Law makers to make suitable amendments to the Information Technology laws to endow the existing legal framework with more teeth.

Cyber laws incorporate various laws relating to:

- Data Protection and Privacy issues (Aadhar being an example)
- Cyber Crimes (Phishing and the recent Wannacry ransomware)
- Intellectual Property(Site Squatters and fake news)

New age Extortions over the www like Wannacry ransomware and the Darknet have compromised the law enforcement process through the deepNet. This is a disturbing situation, in tandem with a report by the Indian Computer Emergency Response Team (CERT-In) which reveals that the incidences of "cyber crimes" in our country has increased around 50 times in the past 3 years. Disturbingly, there were 5284 reported cases of Phishing, 3476 of network probing and 2352 of virus propagation till March 2017.

The twin shields of Data protection and Privacy laws aim at creating a fair balance involving both the privacy rights of the citizens and the interests of data collectors /controllers such as Medical services providers - Hospitals, internet based service providers - emitra, Financial service providers - Banks etc. online frauds related to the financial sector are looming large on the horizon (the HSBC–Denial of Service cyber attack) and in the process kicking off a discussion on the accountability of the Banks themselves for the losses incurred by clients due to such cyber attacks and fraud. In our country the liability is considered in the perspective of due diligence process used by the financial services providers and the PIN and OTP system for access.

Evolving Nature of Cyber Laws

Cyber law is a broad term, which includes all issues, aspects and the legal consequences adherent and relevant to cyber space. Our Country is the 12th nation in the world to have cyber legislation but the IT Act 2000, does not have specific guidelines of electronic payments gateways and there is a segregation of negotiable instruments (as per NI Act, 1881) on the inclusion of the same in the IT Act, which is

having a major consequence on the expansion of e-commerce. The Act aims to empower various government agencies to accept the filing of, creation of and retention of official documents in the digital format. The IT Act introduced the notion of secure digital signatures that will be required to be passed through a structure of security procedures, as per stipulation by the Government.

The Act does provide succor in the form of a statutory remedy to the corporate in case it is proved that the accused had in Act broken into the Network or Computer Systems of the Complainant with the intent of damaging and copying the data. The Act provides for monetary damages, not exceeding Rs. 1 crore ($200,000) in case such charges are proved. The Act has set up the Territorial Jurisdiction of the Adjudicating Officers for cyber crimes and the Cyber Regulations Appellate Tribunal.

In the same vein the Act is mum about the subject of Intellectual Property Rights(IPR), and no provisions have been framed at all for infringements regarding trademarks, copy-rights, patenting of data and information, even of the rights and liabilities of domain name holders are not spelled out which is generally the first step of taking an entry into electronic commerce.

E-Governance has the potential to generate massive benefits in four significant areas:

I) An alteration in the working processes of public institutions and service delivery by government agencies (Electricity, Health, Education etc.).

ii) The encouragement for transparency in government functioning (e-tenders etc.).

iii) The facilitation of useful decentralization (MNREGA etc.).

iv) The augmentation of our strengths for global competitiveness (GST, Ease of doing Business etc.).

While the media used in these transactions are provided by technology, the rules for application and enforcing these transactions are carried out as per Law. In this emergent scenario, it is impossible for the law to exist independent of technology and vice versa.

An Internet Service Provider (ISP) usually handles and manages the website and server hosting services, These Servers may be interweaved between diverse jurisdictions and transmit or exchange information going through a number of geographical areas, as the digital communication is conducted through web and e-connected computers and equipment and this results in end, user identification becoming a task like trying to locate a pin in the haystack.

Insofar as the informational material of the domain is concerned, infringement of trade mark or copyright may be held valid in a court of law provided such written material enjoys copyright or trade-mark protection. While in an ordinary case exceptions to the copyright may be acceptable, this arrangement is open to discussion in the case of web based materials. There is a concomitant issue of determining the apt jurisdiction.

The word “e-government” is open to a number of diverse definitions, depending primarily on perspective, in general it as the provision of governmental services (Education, Health, Law and order) and a process of public administ-ration through the use of ICT. This raises the

issue of legal consequences of the interface between manual and automated resolutions. The problem of clearly demarcating the boundaries between the legal effects of automated decisions as opposed to decisions through the usual executive and judicial decision is also significant.

The provision of legal services to Indian citizens should be separated from judicial functions performed by the Law Courts. The stress of IT Act should be on information and or materials that will develop access to justice for all.

(a) Free-access online to various laws and regulations governing the citizens, the provisions for easier public access to legal materials and counsel in form of online legal aid

(b) Online legal opinions to sustain the provision of free legal aid.

The setting up of appropriate e-governance composition in the form of web portals for availing judicial services, online legal help and aid etc can improve the reach of contact to a host of government services. It will also increase the tempo of use of these services by the citizens. This is a step which will be beneficial not only for the socio-economic well being of the country but also will assist in making better the quality of governance and administering the other government programs.

Privacy Issues

The application of technology to a variety of online transactions has resulted in the crisis of user-identification and personal information theft etc, it is of a grave nature particularly since the transaction is of a remote nature and thus leads to identity theft and a host of other issues a case in point being Credit Card frauds etc.

Data Security

A primary issue is of data Security. It is of extreme significance that the database has to be precise and state-of-the-art security protection should be employed because unauthorized access to the database has severe consequences both for the citizen as well as the government the misuse of the data, leads to pre fraud and having a continuous vigilance of the integrity of electronic data is the only recourse.

Conclusion

E-governance and E-Commerce is not and can never be the complete replacement for the extant systems (that's why we have omni channels). They have to be viewed as a supplement and complement to the existing structures.

Web based commerce and business, with new business models raining like cats and dogs, is the cynosure of all eyes and has also caught the fancy of the cyber criminals who pose a challenge for all stakeholders. The added test is a lack of cyber law implementing enabled manpower and worrisome poor surveillance infrastructure because of the oft criticized 'internal digital divide'. The major troubles are related to the accessible infrastructure which is inclusive of but not limited to frequent connectivity failures, prohibitive cost of internet access (both wireless and wire line) , a deficiency in the suitable legal and regulatory framework in many specific areas of web based commerce are a clear warning of the emerging and well entrenched challenges for IT Laws today.

The extant cyber laws in India are attempting to thwart challenges such as A) The Information Technology Act, 2000 make it obligatory to set up corporate compliance programs including cyber law compliance program in all registered

Corporates. B) The IT 2000 law clearly mandates all registered companies to deploy a relevant IT security policy. C) The Information Technology Act of 2000 provides for further personal liabilities. D) The proper authentication of electronic records and security of data.

The conclusion may be drawn that cyber crime is not a figment of fiction but a real, expanding phenomenon. Furthermore, a steady augmentation in the number of web based crimes is anticipated which demands a far greater consideration of Lawmakers. However, the existing IT and cyber Laws and regulations do not solve the emerging challenges like the Wannacry ransomware attack, various governance issues also cannot be resolved in a jiffy. So the law makers will need to redefine cyber Laws and regulations which are concomitant and relevant to these dynamics.

References

Curran, M. James and Meuter, L. Matthew (2007). Encouraging existing customers to switch to self-service technologies: put a little fun in their lives. Journal of Marketing Theory and Practice, 15 (4), 283–298.

Ganesan R and Vivekanandan K (2009). A Secured Hybrid Architecture Model for Internet Banking (e-Banking). Journal of Internet Banking and Commerce, 14

Koufaris, M. and Hampton-Sosa, W. (2004). The development of initial trust in an online company by new customers. Information & Management, 41 (3), 377-97.

Lee, E.K., Kwon, K.N. and Schumann, D.W. (2005). Segmenting the non-adopter category in the diffusion of internet banking. International Journal of Bank Marketing, 23 (5), 414-37.

Liao, J. and Lin, T. (2008). Effect of consumer charActeristics on their acceptance of online shopping; comparisons among different product types. Computer in human behavior, 24 (1), 48-65.

Malhotra, P. and Singh, B. (2009). Analysis of Internet banking offerings and its determinants in India. Internet Research, 20 (1), 87-106.

Mattila, M., Karjaluoto, H. and Pento, T. (2003). Internet banking adoption among adult customers: early majority or laggards?. Journal of Services Marketing, 17 (5), 514-28.

Rotchanakitumnuai, S. and Spence, M. (2003). Barriers to internet banking adoption: a quantitative study among corporate customers in Thailand. International Journal of Bank Marketing, 21 (6/7), 312-23.

Sayar, C. and Wolfe, S. (2007). Internet banking market performance: Turkey versus the UK. International Journal of Bank Marketing, 25 (3), 122-141.