Cyber Laws and Cyber Security : The Jurisprudence and Judicature

** K. Bhanu Prakash*
*** P. Siva Reddy*

Abstract

With the advancement and use of internet, the number of users have increased manifold. People are using the internet for their daily needs, financial transactions, networking etc. This poses a risk to them if the applications and networks that they are using are not secure enough. They are prone to financial frauds and cyber attacks of various kinds. In this light, it becomes important to have a legal framework to address growing cyber crimes. This paper discusses cyber threats and the legal frameworks that exist in India to deal with the problem.

Keywords: E-mail bombing, EoT, IoT, ransomware, SMAC

I. INTRODUCTION

With the advent of SMAC (Social, Mobile, Analytics and Cloud), IoT (Internet of Things) and EoT (Enterprise of Things), Information Technology (IT) is permeating into every sphere of life. Cyber space allows *Freedom Of Expression* and *Exchange Of Information* besides the diffusion and digitization of activities among individuals and organizations seamlessly. In this technology-driven environment, the estimated value of global financial loss due to cybercrime is approximately €350 and it may increase upto €1.9 trillion by the year 2019.

In India, cyber crimes have grown from ₹ 9,622 crores and ₹ 11,592 crores to ₹ 12,317 crores during 2014, 2015, and 2016 respectively. (Times of India, Jan, 5, 2018). The National Crime Records Bureau (NCRB) and Indian Computer Emergency Report Team (CERT-In) had reported approximately 80 phishing incidents affecting 20 financial organizations, 13 incidents affecting various Automated Teller Machines, Point of Sales systems, and Unified Payments Interface (UPI). The RBI had registered a total of 13,083, 16,468, 13,653, and 12,520 cases of frauds involving credit cards in 2014-2015, 2015 -16, 2016-17, and April-September, 2017 respectively.

Phishing is the biggest single incidence of cyber crime and the impact and incidences of cyber crime have gained momentum in the developed as well as in developing economies.

Globally, cyber crime was perpetrated in the form of phishing, hacking, and dissemination of virus, logic bombs, DoS, e-mail bombing, and spamming, web jacking, Cyber Stalking, Data Diddling, Identity Theft and Credit Card Fraud, Salami Slicing Attack, Software Piracy, and Cloning etc. The 'Black Dot of Death' (IoS Apple), 'Ransomware' (Kill Switch), 'Cyber Caliphate' (ISIS) are some of the cyber attacks. International law is the fundamental and foundation pillar of international order including cyber law and it is still in the embryonic stage.

II. CYBER CRIMES : A TÊTE-À-TÊTE

Cyber incidents are multiplying at a shocking pace and they are ever more becoming difficult causing multiple disruptions in businesses and economies according to Cyber Crime Survey Report by KPMG, 2017. The threats from cyber adversaries are continuing at the same pace, to grow in scale and sophistication. The incidents made distressing damages spanning financial losses, disruption of operational services, erosion of shareholder value and trust.

In India, cyber crime is not defined by either the IT Act, 2000, IT Amendment Act, 2008, or any other

Manuscript received September 14, 2018; revised September 29, 2018; accepted October 5, 2018. Date of publication November 6, 2018.

* K. B. Prakash is Professor with Department of MBA, Godavari Institute Of Engineering and Technology, NH - 16, Chaitanya Knowledge City, Rajahmundry, West Godavari District, Andhra Pradesh, India-533296. (email: bhanucool@yahoo.com)
** P. S. Reddy is Assistant Professor with SMS Department Lakireddy Bali Reddy College Of Engineering (A), Mylavaram, Vijayawada, Krishna District, Andhra Pradesh, India - 521230.(e-mail:siva.podapala@gmai.com)

DOI: 10.17010/ijcs/2018/v3/i6/141445

legislation**.** However, the offense or crime has been defined by the IPC, 1860, as 'any offence or crime in which a computer is used is a cyber crime'. Cyber or computer crimes were defined as unethical, illegal, or unauthorized behaviour of individuals or as groups, relating to the automatic processing and transmission of data, use of computer systems, and networks. **The IT Act, 2000** has 13 chapters and 90 sections (Sec 91 to 94 deals with Amendments to the Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934). The IT Act, 2000 defines the terms *Access*, *Computer, Computer Resource*, *Computer System, Communication Device*, *Data*, *Information*, *Security Procedure* etc. It deals with:

1) legal recognition of electronic documents;
2) digital signatures and their legal recognition;
3) offenses and contraventions;
4) justice dispensation systems for cyber crimes.

The provisions of the **IT Amendment Act, 2008**

1) focus on data privacy and information security;
2) define the term 'cyber café and reasonable security practices to be followed by corporate;
3) Make the technology neutral for digital signature;
4) Rearrange and rewrite the role of intermediaries;
5)Define the role of Indian computer emergency response team, specify clear functions;
6)Include additional cyber crimes like child pornography and cyber terrorism;
7) Authorize an inspector to investigate cyber offences.

According to the IT Act, 2000, cyber crimes can be classified into four types :

1) Cyber crimes *a*gainst individuals;
2) Cyber crimes against property of an individual;
3) Cyber crimes against organizations;
4) Cyber crimes against society at large.

The following are some of the cyber crimes that come under the ambit of cyber crimes against individuals:

1) Harassment through e-mails/messages
2) Cyber-stalking
3) Propagation of obscene material on the internet
4) Defamation
5) Hacking/cracking
6) Indecent exposure.

However, these are considered as cyber crimes against the property of an individual:

1) Computer vandalism
2)Transmitting virus
3) Internet intrusion
4) Unauthorized control over computer system
5) Hacking/cracking are considered as crimes against the property of an individual.

From an organizational point of view, these are some of the cyber crimes:

1) Hacking and cracking
2) Custody of unauthorized information
3) Using cyber terrorism in opposition to the government organization
4) Distribution of pirated software

The following are considered as cyber crimes against the society at large:

1) Pornography (specially child pornography)
2) Spoiling the youth through indecent exposure
3) Trafficking

In order to harmonize internet transactions across the globe, the United Nations Commission on International Trade Law (UNCITRAL) adopted the **Model Law on Electronic Commerce** in 1996. At first, the Budapest Convention on Cybercrime addressed global computer and internet crimes in November, 2001. In India, **E-Commerce Act, 1998** was introduced by the Ministry of Commerce, Government of India. Since later, the Ministry for Information Technology came into being, it was re-drafted and Information Technology Bill, 1999 was placed in the Indian Parliament in December 1999. The **Information Technology (IT) Act, 2000**, passed in May, 2000 was enforced in India with effect from Oct 17, 2000.

III. APPLE iPHONE iOS (11.3) AND iOS 11.4 BETA - FIXING OF THE BUG 'BLACK DOT OF DEATH'

India, with over 462,124,989 internet users is the second largest online market behind China and the share is 13.5% of world internet users. The first hacking incident was evidenced by the world of internet in August, 2017 by the Group Shadow Brokers which targeted the Elite NSA-linked operation known as the Equation Group. Sample of allegedly stolen NSA data was offered by Shadow Brokers. They intended to auction off a bigger trove, following up with leaks. Perhaps, the system failed to identify who were Shadow Brokers and it is still unknown. However, the leaks from different groups have revived debates about the danger of using bugs in commercial products for intelligence gathering.

The financial and economic world was horrified by the strain of Ransomware called WannaCryon on May 12, 2017. It crippled computers in atleast 150 countries and the cost swell into billions of dollars, making it one of the most damaging incidents. It permeated into every sphere, walloping thousands of targets, including public utilities and large corporations. Institutes and service providers such as National Health Service Hospitals and facilities in the United Kingdom were affected by ransomware delaying vital medical procedures, crippling emergency rooms, and creating chaos for many British patients. Software giant Microsoft released the MS17-010 patch for the bug in March, 2017, but many institutions hadn't applied it and were therefore, vulnerable to WannaCry infection. A British security researcher invented a 'KillSwitch' that halted its spread.

The uUsers of Apple iPhone, iPad iOS (11.3), and iOS 11.4 Beta believe that these devices are free from viruses and bugs, and are devoid of all malicious malware, but it is a night mare. iPhone users around the world are being warned about the 'Black Dot of Death' which deletes messages without involvement of the user.

If a user of Apple iPhone opens a message, the iPhone screen goes blank and the bug affects the software as well as other applications on the phone. To fix the bug, it is suggested not to restart the iPhone and to close the i-Message app first. Then tap on 3D Touch Screen on the i-Message app and select new message. Tapping on *Cancel* on the new message screen, redirects back to the list' of iMessage conversations. This is the point of deletion of the message that has a bug.

If the iPhone doesn't support 3D touch, then the following procedure is to be adopted to fix a bug. At first, close the iMessage app and then request the sender to send a reply until the bug goes over the screen in the iMessage. Open iMessage again and tap on back to go to the conversation list. Then delete the thread with the bug from the list.

WhatsAppUsers too were in a spot with the *Text Bomb* bug that could block access to apps and crash the entire smartphone. The bug didn't spare either iPhone or Android users. The problem was first sighted by a Reddit user who claimed that a specially-designed text message with hidden codes could crash many messaging apps including WhatsApp. There was another text bomb that was in the form of a 'Telugu character' which disabled access to iMessage, WhatsApp, Facebook Messenger, Outlook, and Gmail, and also caused the iOS Springboard to crash.

IV. CYBER CRIMES AND CYBER SECURITY : JUDICIAL ENACTMENTS IN INDIA

In Shreya Singhal vs Union Of India, the Supreme Court of India on March 24, 2015 struck down Section 66A of the Information Technology Act, 2000, which is related to restrictions on 'online speech'. It was found unconstitutional on grounds of violating freedom of speech guaranteed under Article 19(1)(a) of the Constitution of India.

IT Act, 2000, Section 66A made it a punishable offence for anyone to send

1) offensive messages through communication service;

2) information which is offensive in nature or has scary character;

3) information which is fake and false but intentionally causes annoyance, criminal intimidation, injury, enmity, inconvenience, insult, obstruction, hatred, danger or ill will, persistently by making use of such computer resource or a communication device.

4) messages through any electronic device for the purpose of causing annoyance or inconvenience or to deceive, or to mislead the recipient about anything or the origin of such messages is punishable with imprisonment for a term which may extend to three years and with fine.

The Supreme Court in Anvar P. V. vs. P. K. Basheer overruled the part of the judgment held by that court in the Nationala Capital Territory of Delhi vs. Navjot Sandhu alias Afsan Guru relating to the admissibility of electronic records. Section 65B of the Indian Evidence Act, 1872 governs the admissibility of secondary evidence of electronic records in general, and as for the bank documents, Section 2(8) of the Banker's Books Evidence Act, 1891, in particular.

V. CYBER SECURITY LAWS : THE FUTURE AHEAD

Globally, cyber law is evolving and the *Cyber Pangea* focuses on coalescing the world through the borderless cyber domain. The US is the first country and India became the twelfth in the world to enact cyber laws. Criminal enforcement against cybercrimes is a prime concern according to Indian Information Technology Act, 2000. Cyber Security and Cyber Policy regulations and enactments focus on interplay of cyber policies with the constitutional precepts, cybercrime, and electronic evidence to IPR and contracts. As the internet gets increasingly sophisticated, criminology and cybercrime are opening up more career avenues. India needs cybercrime awareness clinics.

Cybercrime is a menace and to curb it a comprehensive cyber crime penal code covering investigation, prosecution, and adjudication is imminent. The cohesive efforts, coordination, and co-operation among developed and developing nations are required to mitigate cyber crimes. Consistent and conscious efforts to deal with cyber security are the dire need to establish a robust cyber security framework that is aligned to address regulatory requirements. Some of the cyber risk mitigating strategies *inter alia* include cyber awareness (gaming, cyber drills, and situational videos), cyber security risk assessment, and measurement systems, emergency cyber responsive framework, incident response, and digital brand protection. The concept of *cyber insurance* also reduces cyber vulnerability as well as financial loss.

India, a digital economy has taken steps to build resistance against cyber security threats and promoting cyber resilience framework. The guidelines relate to
1) Cyber security framework for banks on June, 2016;
2) IT Framework for NBFCs on June, 2017;
3) Guidelines on information and cyber security for insurers in April, 2017;
4) Cyber security and cyber resilience framework of stock exchanges in July, 2015 ;
5) Cyber security and cyber resilience framework for registrars to an Issue/Share Transfer Agents in September, 2017;
6)General guidelines of Department Of Telecommunications (DOT) in May, 2017; and
7) Central electricity authority for reviewing the needs of cyber security in critical infrastructure support.

The traditional approach to jurisdiction invites a court to ask whether it has the territorial, pecuniary, or subject matter jurisdiction to entertain the case before it. When using internet without any restrictions around the globe, there will be a paradigm of territorial control. Unless and until there is a comprehensive cyber law that addresses the penalties and punishments for cyber crimes, the suffering of thousands of silent victims will remain.

REFERENCES

[1] P. Agarwal, Inform. security and cyber laws, 2010. India: ACME Learning Pvt. Ltd.

[2] A. Chauhan, “Evolution and development of cyber law : A study with special reference to India," 2013.

[3] A. Edappagath, "Cyber laws and enforcements to optimize benefits of ICT," *I-WAYS, Dig. of Electron. Commerce Policy and Regulation*, vol. *27*, no. *3,4,* 2004.

[4] Indian Inst. of Banking and Finance, *Cyber Laws in India*. New Delhi: TaxMann Publishers.

[5] C. John, "iPhone users beware: The 'block dot of death' is out to get you," May 14, 2018. [Online]. Available: https://www.thequint.com/tech-and-auto/tech-news/iphone-black-dot-of-death-bug-crashing-message-application

[6] S. Katkuri, "Indian Cyber Law," *Int. J. of Advanced Res. and Develop*., vol. *3*, no. *1*, pp. 640-644, 2018.

[7] KPMG, "IndiaTrends2018: Trends shaping digital India," 2018. [Online]. Available: https://home.kpmg/in/en/home/insights/2018/05/digital-payments-robotics-ecommerce-health-tech.html

[8] KPMG, "Cyber crime survey report insights and perspectives," 2017. [Online]. Available: https://assets.kpmg/content/dam/kpmg/in/pdf/2017/12/Cyber-Crime-Survey.pdf

[9] N. Kshetri, "Diffusion and effects of cyber-crime in developing economies," *3rd World Quart.*, vol. *31*, no. *7*., pp. 1057-1079, 2010.

[10] A.P. Kumar, Cyber law - A view to social security, 2009, India: YFI.

[11] N. S. Nappinai, *Technol. Laws Decoded*, 2018. New York: LexisNexis Publications.

[12] P. K. Paul and P. S. Aithal, "Cyber crime: Challenges, issues, recommendation, and suggestion in Indian context," *Int. J. of Advanced Trends in Eng. and Technol.*, *3*(1), pp. 59-62, 2018.

[13] PriceWaterhouseCoopers, "Strengthening digital society against cyber shocks," 2018. [Online]. Available:

www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-

[14] PriceWaterhouseCoopers, "Revitalizing privacy and trust in a data-driven world,” 2018. [Online]. Available: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/revitalizing-privacy-trust-in-data-driven-world.html

[15] PTI, "Cyber crimes rose between 2014 and 2017," 2018. [Online]. Available: https://timesofindia.indiatimes.com/business/india-business/cyber-crimes-rose-between-2014-and-2017-govt/articleshow/62380670.cms

[16] A. Sarmah and R. Sarmah, "A brief study on cyber

crime and cyber laws of India," *Int. Res. J. of Eng. and Technol.*, vol. *4*, no. *6*, 2018.

[17] N. Strossen, "Cybercrimes vs. cyber liberties," *Int. Rev. of Law Comput. & Technol*., vol.*14*, no. *1*, pp. 11-14, 2000.

[18]Internet Live Stats [Online]. Available: www.internetlivestats.com/internet-users/india/

[19] Teckall, "iPhone users beware! The 'Black dot of death is out to get you," 2018. [Online]. Available: ttp://teckall.com/iphone-users-beware-the-black-dot-of-death-is-out-to-get-you/

[20] B. Venkatesh, "India needs cybercrime awareness clinics," April 29, 2018. [Online]. Available: https://www.thehindu.com/education/india-needs-cybercrime-awareness-clinics/article23706912.ece

About the Authors

Dr. K. Bhanu Prakash is Professor with the Department MBA (A), Rajamahendravaram. He is also acting as Chief Financial Officer for Mohan Nandan Infra (MN Infra), Tadepalligudem, West Godavari. He completed doctoral fegree from Acharya Nagarjuna University in 2012.

Siva Reddy has been working with School of Management Studies, Lakireddy Bali Reddy College of Engineering (A) from 2015 . He is pursuing his Doctoral Degree in Acharya Nagarjuna University, in the area of Finance. He has diversified experience in corporate world as well as in academics. He specialized in Finance, particularly in the area of Financial Derivatives and Security Analysis.