COMPARATIVE ANALYSIS OF HACKING LAWS IN INDIA WITH UNITED STATES AND UNITED KINGDOM

Esmahan F. Alakab Khaniefr*

"When a man is denied the right to live the life he believes in, he has no choice but to become an outlaw." - Nelson Mandela

INTRODUCTION

Crime, in modern times this term doesn't have any universally accepted definition, but one can define crime, also called an offence as an act harmful not only to some individual, but also to the community or the state also known as public wrong. Such acts are forbidden and punishable by law. What is a criminal offence is defined by criminal law of each country. While many countries have a crime catalogue known as the criminal code however in some common law countries no such comprehensive statute exists.

The state has the power to severely restrict one's liberty for committing a crime. Modern societies therefore adopt and adhere a criminal procedure during the investigation and trial of the offence and only if found guilty, the offender may be sentenced to various punishments, such as life imprisonment or in some jurisdictions like in India even death.

To be classified as a crime, the act of doing something bad also called as actusreus must be usually accompanied by the intention to do something bad i.e. mens rea, with certain exceptions like strict liability.

Cybercrime is any criminal activity in which a computer or network is the source, target or tool or place of crime. According to The Cambridge English Dictionary cybercrimes are the crimes committed with the use of computers or relating to computers, especially through the internet. Crimes which involve use of information or usage of electronic means in furtherance of crime are covered under the ambit of cybercrime. Cyber space crimes may be committed against persons, property, government and society at large.

HACKING & ITS TYPE

Hacking

* *Research Scholar* @ Dept. of Legal studies & Research, Acharya Nagarjuna University, Guntur, (A.P.)

"An unauthorized user who attempts to or gains access to an information system is known as hacker. Hacking is a cybercrime even if there is no visible damage to the system, because it is an invasion in to the privacy of data."

- **White Hat Hackers**

  "*They are those hackers who believe that information sharing is good, and that it is their duty to share their expertise by facilitating access to information. However there are some white hat hackers who are just "joy riding" on computer systems*."
- **Black Hat Hackers**

  "*Black hat hackers cause damage after intrusion. They may steal or modify data or insert viruses or worms which damage the system. They are also known as crackers*."
- **Grey Hat Hackers**

  "*These types of hackers are typically ethical but occasionally they can violate the hacker ethics. They will hack into networks, stand-alone computers and software. Network hackers try to gain unauthorized access to private computer networks just for challenge, curiosity, and distribution of information*."

Indian Laws on Hacking

To sum up, though a crime-free society is Utopian and exists only in dream-land, it should be constant endeavour of rules to keep the crimes lowest.[1] Especially in a society that is dependent more and more on technology, crime based on electronic offences are bound to increase and the law makers have to go the extra mile compared to the fraudsters, to keep them at bay. Technology is always a double-edged sword and can be used for both the purposes – good or bad. Steganography, Trojan Horse, Scavenging (and even DoS or DDoS) are all technologies and per se not crimes, falling into wrong hands with a criminal intent who are out to capitalize them or misuse them, they come into the gamut of cybercrime and become punishable offences. Hence, it should be the persistent efforts of rulers and law makers to ensure that technology grows in a healthy manner and is used for legal and ethical business growth and not for committing crimes.[2]

[1] Aarseth, Espen. 1997. *Cybertext: Perspectives on ergodic literature*, Baltimore: Johns Hopkins University Press

[2] Abbate, Janet; *Privatizing the Internet: Competing visions and chaotic events*, 1987–1995. *IEEE Annals of the History of Computing* 32(1): pp.10-22

IT legislation in India: Mid 90's saw an impetus in globalization and computerization, with more and more nations computerizing their governance, and e-commerce seeing an enormous growth. Previously, most of international trade and transactions were done through documents being transmitted through post and by telex only. Evidences and records, until then, were predominantly paper evidences and paper records or other forms of hard-copies only. With much of international trade being done through electronic communication and with email gaining momentum, an urgent and imminent need was felt for recognizing electronic records i.e. the data what is stored in a computer or an external storage attached thereto. The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations passed a resolution in January 1997 inter alia, recommending all States in the UN to give favorable considerations to the said Model Law, which provides for recognition to electronic records and according it the same treatment like a paper communication and record.

Objectives of I.T. legislation in India: It is against this background the Government of India enacted its Information Technology Act 2000 with the objectives as follows, stated in the preface to the Act itself. "to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."[3]

CONSTITUTIONAL LIABILITY

Hacking into someone's private property or stealing some one's intellectual work is a complete violation of his right to privacy. The Indian constitution does not specifically provide the "right to privacy" as one of the fundamental rights guaranteed to the Indian citizens but it is protected under IPC.

Right to privacy is an important natural need of every human being as it creates boundaries around an individual where the other person's entry is restricted. The right to privacy

[3] Bertsch, Gary K. (ed.). 1988. *Controlling East–West trade and technology transfer: Power, politics, and policies*, Durham: Duke University Press.

prohibits interference or intrusion in others private life. The apex court of India has clearly affirmed in its judicial pronouncements that right to privacy is very much a part of the fundamental right guaranteed under Article 21 of the Indian constitution.

Thus right to privacy is coming under the expended ambit of Article 21 of Indian constitution. So whenever there is some cybercrime which is related to the persons private property or its personal stuff then the accused can be charged of violation of Article 21 of Indian constitution, and prescribed remedy can be invoked against the accused.

CRIMINAL LIABILITY

Criminal liability in India for cybercrimes is defined under the Indian Penal Code (IPC). Certain Following sections of IPC deal with the various cybercrimes, Such as Sending threatening messages by e-mail (Sec .503 IPC), Word, gesture or act intended to insult the modesty of a woman (Sec.509 IPC), Sending defamatory messages by e-mail (Sec .499 IPC), Bogus websites, Cyber Frauds (Sec .420 IPC), E-mail Spoofing (Sec .463 IPC), Making a false document (Sec.464 IPC), Forgery for purpose of cheating (Sec.468 IPC) etc..[4]

The applications of these sections are subject to the investigating style of investigating officer and charge sheet filed by the investigating agency and nature of cybercrime. In India there are number of cases filed under these IPC provisions related to the cybercrime. According to the report of Home Ministry, in 2012 there are 601 cases filed under the various provisions of IPC.

UNITED STATES LAWS

Cybercrimes run the gamut-from student mischief to international terrorism. The increasingly severe penalties for these types of crimes serve as deterrents as more people become aware of the consequences they might face. Cybercrime causes major losses of time, money, and good reputations, and judges and prosecutors have no choice but to treat these crimes with utmost severity. Substantive laws include crimes such as online gambling, child pornography, theft of intellectual property, fraud, and identity theft.[5]

[4] Ceruzzi, Paul E. 1996. From scientifi c instrument to everyday appliance: The emergence of personal computers, 1970–77. *History and Technology* 13(1): 1-31.
[5] Id.

The Computer Fraud and Abuse Act (CFAA)[6] was enacted by Congress in 1986 as an amendment to existing computer fraud law (18 U.S.C. § 1030), which had been included in the Comprehensive Crime Control Act of 1984. The law prohibits accessing a computer without authorization, or in excess of authorization.

The original 1984 bill was enacted in response to concern that computer-related crimes might go unpunished. The House Committee Report to the original computer crime bill characterized the 1983 techno-thriller film War Games in which a young Matthew Broderick breaks into a U.S. military supercomputer programmed to predict possible outcomes of nuclear war and unwittingly almost starts World War III-as *"a realistic representation of the automatic dialing and access capabilities of the personal computer."*[7]

The CFAA was written to increase the scope of the previous version of 18 U.S.C. § 1030 while, in theory, limiting federal jurisdiction to cases *"with a compelling federal interest-i.e., where computers of the federal government or certain financial institutions are involved or where the crime itself is interstate in nature."* In addition to amending a number of the provisions in the original section 1030, the CFAA also criminalized additional computer-related acts. Provisions addressed the distribution of malicious code and denial of service attacks. Congress also included in the CFAA a provision criminalizing trafficking in passwords and similar items.[8] Since then, the Act has been amended a number of times-in 1989, 1994, 1996, in 2001 by the USA PATRIOT Act, 2002, and in 2008 by the Identity Theft Enforcement and Restitution Act.[9]

In January 2015 Barack Obama proposed expanding the CFAA and the RICO Act in his Modernizing Law Enforcement Authorities to Combat Cyber Crime proposal.[10] DEF CON organizer and Cloudflare researcher Marc Rogers, Senator Ron Wyden, and Representative Zoe Lofgren have stated opposition to this on the grounds it will make many regular Internet

[6] Jarrett, H. Marshall; Bailie, Michael W; Available at: www.justice.gov/criminal/cybercrime/doc/ccmanual.pdf; (Accessed on 03/06/2017)

[7] *H.R. Rep. 98-894, 1984 U.S.C.C.A.N. 3689, 3696 (1984)*

[8] Available at: https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat (Accessed on 03/01/*2017*

[9] Cooke, Claudia. 1983b. User of the month: Taking the strain out of calculating wages. Sinclair User, August, 78–79.

[10] Available at: http://www.huffingtonpost.in/entry/obama-hackers_n_6511700 (Accessed on 30/01/2017)

activities illegal, and moves further away from what they were trying to accomplish with Aaron's Law.[11]

UNITED KINGDOM

The hacking of computers is a crime which has increased exponentially since the inception of the internet. It takes many forms: from the defrauding of large corporations, the hacking of government databases to expose state secrets, to the identity theft of individuals.[12]

THE COMPUTER MISUSE ACT 1990

The Computer Misuse Act 1990 (CMA 1990) was introduced in August 1990 following a Law Commission report surrounding computer misuse which found that the UK was trailing behind many EU member states in relation to technological development.

WHAT OFFENCES WERE INTRODUCED BY CMA 1990?

CMA 1990 introduced the following three new offences into UK criminal law:

- unauthorized access to computer material;
- unauthorized access with intent to commit a further offence;
- unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer, etc. (as amended by the Police and Justice Act 2006).

UNAUTHORIZED ACCESS TO COMPUTER MATERIAL

The basic notion of hacking – whereby an individual causes a computer to perform a function when at the time he intends to access a program or data held in a computer – is covered by the offence of unauthorized access to computer material (s 1, CMA 1990).[13]

Does an individual have to know that his accessing the computer material is unauthorized?

[11] Available at: https://www.usnews.com/news/articles/2015/01/27/obama-goodlatte-seek-balance-on-cfaa-cybersecrity, (Accessed on 30/01/2017)

[12] Curtis, Glenn E. 1990. *Yugoslavia: A country study* . Washington, DC: Library of Congress, Federal Research Division.

[13] Id.

For the offence to occur the access to the computer material has to be unauthorized and the individual gaining access has to be aware that his access is unauthorized.[14]

What is meant by computer material?

There is no definition of computer material within CMA 1990. This has allowed CMA 1990 to apply to new pieces of technology as and when they are developed.[15] However, the accepted definition of computer being any device for storing and processing information can be found in the Civil Evidence Act 1968.[16]

UNAUTHORIZED ACCESS WITH INTENT TO COMMIT A FURTHER OFFENCE

Section 2 of CMA 1990 covers unauthorized access to computer material with the intent to commit or facilitate the commission of further offences. The basis notion is that someone guilty of an offence under sec. 1 of CMA 1990 will have further criminal sanctions imposed on him if this is done with the intention to commit or facilitate the commission of further offences.

What is meant by further offences under section 2?

Further offences under section 2 are those which have a sentence fixed by law or where an individual found guilty of that offence would be liable for a term of imprisonment of five years or more.

Examples of a further offence may be:

- fraud under the Fraud Act;
- forgery or counterfeiting under the Forgery and Counterfeiting Act 1981;
- theft under the Theft Act 1968;
- criminal damage under the Criminal Damage Act 1971.

[14] Hafner, Katie, and John Markoff. 1991. *Cyberpunk: Outlaws and hackers on the computer frontier*, London: Touchstone.

[15] Haddon, Leslie. 1992. Explaining ICT consumption: The case of the home computer. In *Consuming technologies: Media and information in domestic spaces*, ed. R. Silverstone and E. Hirsch, 82–96, London: Routledge.

[16] Janjatović, Petar. 1998. *IlustrovanaEnciklopedija Yu Rocka 1960–1997* . Belgrade: Geopoetika

Unauthorized acts with intent to impair

Section 3 of CMA 1990 was amended by the Police and Justice Act 2006. Its aim was to tackle computer viruses and denial of service attacks, which can have devastating effects on the organisations targeted. The offence does not have to be against a particular computer, program or data and is committed even if, for example, the denial of service is only temporary.[17]

OTHER AMENDMENTS TO CMA 1990

The Serious Crime Act 2015 added a new offence (s 3ZA) of 'unauthorized acts causing, or creating risk of, serious damage'. The territorial scope of computer misuse was also extended, meaning that a UK national is still committing an offence if the computer misuse happened outside the UK, as long as it was also illegal in the country where the hacking took place.[18] The Police and Justice Act 2006 added a new offence of 'making, supplying or obtaining articles for use in offence under ss 1, 3 or 3ZA' (s 3A).

PENALTIES

Penalties for offences under CMA 1990 range from two years' imprisonment and/or a fine for unauthorized access to computer material; up to five years and/or a fine for unauthorized access with intent to commit or facilitate commission of further offences; up to 10 years and/or a fine for unauthorized modification of computer material; and imprisonment for life and/or a fine for breach of s 3ZA.

OTHER LEGISLATION DEALING WITH COMPUTER HACKING

The Terrorism Act 2000

When the Terrorism Act 2000 (TA 2000) first came into force it made the threat of or use of computer hacking a potential act of terrorism.

The use or threat of an action designed seriously to interfere with or seriously to disrupt an electronic system will be a terrorist action under TA 2000 only if both of the following

[17] Janjatović, Petar. 1998. *IlustrovanaEnciklopedija Yu Rocka 1960–1997*, Belgrade: Geopoetika

[18] Kent, Steven L. 2001. *The ultimate history of video games: From Pong to Pokémon and beyond: The story behind the craze that touched our lives and changed the world*, New York: Three Rivers Press.

conditions are satisfied, 1) It is designed to influence the government or to intimidate the public or a section of the public and 2) It is made for the purpose of advancing a political, religious or ideological cause.

TA 2000 does not, however, make for additional penalties for hackers who would be punished under the existing laws of CMA 1990.[19]

CONCLUSIONS

Cybercrime is a new form of crime that has emerged due to computerization of various activities in an organization in a networked environment. With the rapid growth of information technology cybercrimes are a growing threat. Technology has a negative aspect as it facilitates commercial activity. Ordinarily the law keeps pace with the changes in technology but the pace of technological developments in the recent past, especially in the field of information and technology is impossible to keep pace with legal system. An important concern relates to modernizing penal laws of many countries which predate the advent of computers. On the one hand, the existing laws have to be change to cope with the computer related fraud such as hacking, malicious falsification or erasure of data, software theft, software attacks etc. and on the other, new legislation is also necessary to ensure data protection and piracy. The need for a law on data protection is paramount if India is to sustain investor confidence, especially among foreign entities that send large amounts of data to India for back-office operations. Data protection is essential for outsourcing arrangements that entrust an Indian company with a foreign company's confidential data or trade secrets, and/or customers' confidential and personal data.

Also in the above chapters we have talked about the Indian police system for cybercrimes which is subjected to the improvisation, and a new and clear specific legislation which can fight easily against the cybercrimes. Further the proposed initiatives and amendments by government to the IT act, which are likely to be implemented, soon will be implemented as soon as possible. The proposed amendments widen the liability for breach of data protection and negligence in handling sensitive personal information. Additionally, the Government of India, with the help of the Department of Information Technology, is currently working on a holistic law on data protection based on the European Union directive. Further, the

[19] Kent, Steven L. 2001. *The ultimate history of video games: From Pong to Pokémon and beyond: The story behind the craze that touched our lives and changed the world* . New York: Three Rivers Press.

government plans to create a "Common Criterion Lab," backed by the Information Security Technical Development Council, where intensive research in cryptography and product security can be undertaken. As Prevention is always better than cure, a smart internet user should take certain precautions while operating the internet and should follow certain preventive measures for cybercrimes; these measures can be considered as suggestions also:

- A person should never send his credit card number to any site that is not secured, to guard against frauds.
- One should avoid disclosing any personal information to strangers via e-mail or while chatting.
- One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.
- It is always the parents who have to keep a watch on the sites that your children are accessing, to prevent any kind of harassment or depravation in children.
- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.
- Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens (cybercitizen or an entity or person actively involved in online communities and a user of the Internet).
- Web servers running public sites must be physically separately protected from internal corporate network.
- An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.
- It is better to use a security program by the body corporate to control information on sites.

- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.

- As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.

- Special police task force which is expert in techno field will be constituted.