International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 01-08-2023, Accepted: 16-08-2023, Published: 01-09-2023
Volume 5, Issue 3, 2023, Page No. 87-90

Growth of cybercrimes and legislative endeavours in India

Manoj Kumar Sadual[1], Ankit Sourav Sahoo[2]
[1] Associate Professor, Department of Law, Utkal University, Bhubaneswar, Odisha, India
[2] Assistant Professor, Department of Law, Lajpat Rai Law College, Sambalpur University, Sambalpur, Odisha, India

Abstract
With the rapid development of computer technology and internet over the years, the problem of cyber crime has assumed gigantic proportions and emerged as a global issue. It has created an entirely new set of problems for law enforcement agencies all over the world. It has equally become cause of serious concern for the legal fraternity to find effective ways and means to combat cyber criminality because of its worldwide devastating effect. Cyber security provides protection to the internet connected networks and system from the cyber-attacks. To stop attacks everyone must know and aware of all cyber law, regulations and compliance to secure the cyber. Cyber security is all about to stop cyber-crime. Cyber security is must and we have to know about all safety measures required to stop cyber-crime. Securing online information is priority where everyone is involved with technology. Whenever anyone talked about cyber security, straight one thing comes in mind that is cyber-crime and what safety measures need to take to be safe from it. Various legal regimes have tried their best to bring provisions to combat the issue.

Keywords: Cybercrimes, cyberspace, global perspective, digital future, cybersecurity, legal frameworks

Introduction
The rapid growth of digital technology has facilitated unprecedented opportunities for communication, commerce, and innovation. However, alongside these benefits, cyber-crimes have also proliferated, posing significant challenges to global security. This journal article delves into the nature and prevalence of cyber-crimes, their impact on national and international security, and the legal hurdles faced in combating this ever-evolving threat Cybercrime is a relatively new type of crime in the world. Cybercrime is the most common crime in modern India, and it has a terrible impact. Criminals not only cause significant damages to society and the government, but they also disguise their identities to a large extent. A variety of unlawful acts are carried out by technically proficient criminals over the internet. In a broader sense, cybercrime can be defined as any illicit conduct in which a computer or the internet is used as a tool, a target, or both. The role of the internet's global significance has enhanced and its impact is enormous. The impact of the internet is growing and has increased the Cybercrime is any illegal activity which is committed through a computer network, the internet. Cyber-crime involves the interruption of privacy, or damage to the computer system properties such as files, website pages or software. With the gradual development of Cybercrimes, UN and India have tried to address the issue at their own levels through various mechanisms.

Development of cybercrimes in global context
On the advent of a large number of cyber crimes, many nations have felt the need to have some control mechanism. In order to combat the challenges posed by cybercrime, many countries have beefed themselves up against such crime. A number of countries have introduced extensive amendments to their substantive criminal law. These are USA, Austria, Denmark, France, Germany, Greece, Finland, Italy, Turkey, Sweden, Switzerland, Australia, Canada and Japan. The United States especially has made numerous amendments to their existing legislation. India, Spain, Portugal, UK, Malaysia and Singapore have made new enactment to prevent computer-related crime. Apart from fine, the punitive deterrents range from imprisonment from one year to ten years depending upon the gravity of the offence. Unauthorized access to computer/data/program has been classified as computer crime/offence by almost all the countries that have either enacted new statutes or amended existing criminal laws. Many countries have commenced to enact laws related to Digital Signature. The Convention on Cybercrime at Budapest was the first-ever international treaty on criminal offences committed against or with the help of computer networks such as the internet. The Convention deals in particular with offences related to infringements of copyright, computer-related fraud, child pornography and offences connected with network security. It also covers a series of procedural powers such as searches of an interception of material on computer networks. Its main aim, as set out in the Preamble, is to pursue "a common criminal policy aimed at the protection of society against cybercrime, inter-alia by adopting appropriate legislation and fostering international cooperation [1]." It has an Additional Protocol making it a criminal offence to disseminate racist or xenophobic propaganda via computer networks. The treaty has a threefold aim: to lay down common definitions of certain criminal offences relating to the use of the new technologies, to define methods for criminal investigations and prosecution, and to define methods for international communication. The criminal offences concerned are: those committed against the confidentiality, integrity and availability of computer data or systems (such as the spreading of viruses); computer-related offences (such as virtual fraud and forgery); content-related offences (such as the possession and intentional distribution of child pornography); offences related to infringements of intellectual property and related rights. Another objective is

to facilitate the conduct of criminal investigations in cyberspace, thanks to a number of procedural powers, such as the powers to preserve data, to search and seize, to collect traffic data and to intercept communications [2].

The European Union has set up an agency to coordinate work to combat the rising tide of cybercrime. The European Network and Information Security Agency will help educate the public about viruses, hacker attacks and other security problems. It will also act as a coordinator for Europe-wide investigations into virus outbreaks or electronic attacks [3].

Most Western countries have initiated some kind of anti-cybercrime capability or legislation, but this is slow to develop. In 1997 the UK established the Internet Crime Forum, bringing together police, government, prosecutors, internet industry officials and lawyers to discuss issues of mutual concern Canada looks likely to follow suit in light of the May 2000 G-8 meeting on cybercrime. Many other computer crime units are being established around the world. The FBI, for example, established its C-37 unit in 1996; the Russian Federal Security Service has established a system to monitor e-mail codenamed SORM (System of Operational and Investigative Measures). The G-8 currently has a high-tech crime group developing best practices for investigating online crime. The Council of Europe has drafted a convention on cybercrime, which aims to enhance powers to investigate and prosecute cybercrimes.

More than 100 countries do not have the laws to deal with computer-related crime, including at least 60% of Interpol members. This has a huge impact on a country's own ability to combat cybercrime and on its ability' to assist other countries with their investigations. The hampering of the US-Philippine hunt for the perpetrator of the 'I Love You' virus was a prime example of this. There is a clear need to establish special communication channels that should always be open to process urgent and critical cases, as well as to enhance intelligence cooperation and coordination worldwide. The country's authorities at the UN digital summit have defended Iran's policy of blocking access to certain websites. Iranian authorities claim only sites not compatible with Islam are blocked [4].

Efforts made by the United Nations

Following the Seventh UN congress on the Prevention of Crime and the Treatment of Offenders, which took place in 1985, the Secretary-General prepared a report entitled "Proposals for Concerted International Action Against Forms of Crime Identified in Milan Plan of Action. Computer Crime was discussed in paragraphs 42-44 of that report. At the 12th plenary meeting of the Eighth Congress, in 1990, Canada introduced a draft resolution on computer crimes on behalf of 21 sponsors. At its 13th plenary meeting, the Congress adopted the resolution, which, inter alia, called upon member States to intensify their efforts to combat computer crimes by considering, if necessary, the following measures:

1. "Modernisation of national criminal laws and procedures, including measures to:
   - Ensure that existing offences and laws concerning investigative powers and admissibility of evidence in judicial proceedings adequately apply and, if necessary, make appropriate changes;
   - In the absence of laws that adequately apply, create offences and investigative and evidentiary procedures, where necessary, to deal with this novel and sophisticated form of criminal activity;
   - Provide for the forfeiture or restitution of illegally acquired assets resulting from the commission of computer-related crimes;
2. Improvement of computer security and prevention measures, taking into account the problems related to the protection of privacy, the respect for human rights and fundamental freedoms and any regulatory mechanisms pertaining to computer usage;
3. Adoption of measures to sensitize the public, the judiciary and law enforcement agencies to the problem and the importance of preventing computer-related crimes;
4. Adoption of adequate training measures for judges, officials and agencies responsible for the prevention, investigation, prosecution and adjudication of economic and computer-related crimes;
5. Elaboration, in collaboration with interested organisations, of rules of ethics in the use of computers and the teaching of these rules as part of the curriculum and training in informatics;
6. Adoption of policies for the victims of computer-related crimes which are consistent with the UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, including the restitution of illegally obtained assets, and measures to encourage victims to report such crimes to the appropriate authorities."

Acts amended by information technology act, 2000

The Indian penal code, 1860

Normally referred to as the IPC, this is a very powerful legislation and probably the most widely used in criminal jurisprudence, serving as the main criminal code of India. Enacted originally in 1860 and amended many time since, it covers almost all substantive aspects of criminal law and is supplemented by other criminal provisions. In independent India, many special laws have been enacted with criminal and penal provisions which are often referred to and relied upon, as an additional legal provision in cases which refer to the relevant provisions of IPC as well. ITA 2000 has amended the sections dealing with records and documents in the IPC by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc) have since been amended as electronic record and electronic document thereby bringing within the ambit of IPC, all crimes to an electronic record and electronic documents just like physical acts of forgery or falsification of physical records. In practice, however, the investigating agencies file the cases quoting the relevant sections from IPC in addition to those corresponding in ITA like offences under IPC 463,464, 468 and 469 read with the ITA/ITAA Sections 43 and 66, to ensure the evidence or punishment stated at least in either of the legislations can be brought about easily.

The Indian evidence act 1872

This is another legislation amended by the ITA. Prior to the passing of ITA, all evidences in a court were in the physical form only. With the ITA giving recognition to all electronic records and documents, it was but natural that the evidentiary legislation in the nation be amended in tune with

it. In the definitions part of the Act itself, the "all documents including electronic records" were substituted. Words like 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the ITA, were all inserted to make them part of the evidentiary mechanism in legislations. Admissibility of electronic records as evidence as enshrined in Section 65B of the Act assumes significance. This is an elaborate section and a landmark piece of legislation in the area of evidences produced from a computer or electronic device.

Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be treated like a document, without further proof or production of the original, if the conditions like these are satisfied:

a. The computer output containing the information was produced by the computer during the period over which the computer was used regularly by lawful persons.
b. The information derived was regularly fed into the computer in the ordinary course of the said activities;
c. Throughout the material part of the said period, the computer was operating properly and a certificate signed by a person responsible, etc.

To put it in simple terms, evidences (information) taken from computers or electronic storage devices and produced as print-outs or in electronic media are valid if they are taken from system handled properly with no scope for manipulation of data and ensuring integrity of data produced directly with or without human intervention etc and accompanied by a certificate signed by a responsible person declaring as to the correctness of the records taken from a system a computer with all the precautions as laid down in the Section. However, this Section is often being misunderstood by one part of the industry to mean that computer print-outs can be taken as evidences and are valid as proper records, even if they are not signed. We find many computer generated letters emanating from big corporates with proper space below for signature under the words "Your faithfully" or "truly" and the signature space left blank, with a Post Script remark at the bottom "This is a computer generated letter and hence does not require signature". The Act does not anywhere say that 'computer print-outs need not be signed and can be taken as record'.

The bankers' books evidence (BBE) act, 1891

Amendment to this Act has been included as the third schedule in ITA. Prior to the passing of ITA, any evidence from a bank to be produced in a court, necessitated production of the original ledger or other register for verification at some stage with the copy retained in the court records as exhibits. With the passing of the ITA the definitions part of the BBE Act stood amended as: "'bankers ' books' include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device". When the books consist of printouts of data stored in a floppy, disc, tape etc, a printout of such entry certified in accordance with the provisions to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons; the safeguards adopted to prevent and detect unauthorized change of data to retrieve data that is lost due to systemic failure or In short, just like in the Indian Evidence Act, the provisions in Bankers Books Evidence Act make the printout from a computer system or a floppy or disc or a tape as a valid document and evidence, provided, such print-out is accompanied by a certificate stating that it is a true extract from the official records of the bank and that such entries or records are from a computerized system with proper integrity of data, wherein data cannot be manipulated or accessed in an unauthorized manner or is not lost or tamperable due to system failure or such other reasons. Here again, let us reiterate that the law does not state that any computerized print-out even if not signed, constitutes a valid record. But still even many banks of repute (both public sector and private sector) often send out printed letters to customers with the space for signature at the bottom left blank after the line "Yours faithfully" etc and with a remark as Post Script reading: "This is a computer generated letter and hence does not require signature". Such interpretation is grossly misleading and sends a message to public that computer generated reports or letters need not be signed, which is never mentioned anywhere in nor is the import of the ITA or the BBE. The next Act that was amended by the ITA is the Reserve Bank of India Act, 1934. Section 58 of the Act sub-section (2), after clause (p), a clause relating to the regulation of funds transfer through 15 electronic means between banks (i.e. transactions like RTGS and NEFT and other funds transfers) was inserted, to facilitate such electronic funds transfer and ensure legal admissibility of documents and records therein.

Reserve bank of India act, 1934

The Information Technology Act, 2000 has made some amendments in Reserve Bank of India Act, 1934. These amendments have been made in the manner specified in the Fourth Schedule read with section 94. In section 58, sub clause pp is inserted after clause (p) of subsection 2 with the purpose to introduce and regulate Electronic Fund Transfer (EFT) mechanism between the banks and other financial institutions.

New endeavours by the information technology act, 2000

The Act ensures for infrastructure for safe promotion and growth of electronic commerce. Prior to the coming into effect of the IT Act, 2000, the judiciary in India was reluctant to accept electronic records and communications as evidence. Even email was not accepted under the prevailing statutes of India as an accepted legal form of communication and as evidence in a court of law. The IT Act, 2000 changed this scenario by legal recognition of the electronic format. Indeed, the IT Act, 2000 is a step forward. From the perspective of the corporate sector, the IT Act 2000 and its provisions contain the following positive aspects:

1. The implications of these provisions for the corporate sector are that email is now be a valid and legal form of communication in our country, which can be duly produced and proved in a court of law. The corporates today thrive on email, not only as the form of communication with entities outside the company but also as an indispensable tool for intra company

communication. Corporates ought to understand that they shall need to be more careful while writing emails, whether outside the company or within, as emails, in whatever language, could be proved as a legal document in a court of law, sometimes to the detriment of the company. Even intra company notes and memos, till now used only for official purposes, shall come within the ambit of the IT Act, 2000 and will be admissible as evidence in a court of law. A lot would of course depend upon how these emails are-proved in a court of law.

2. Companies shall be able to carry out electronic commerce using the legal infrastructure provided by the IT Act, 2000. Till the coming into effect of the Indian cyber law, the growth of electronic commerce was impeded in our country basically because there was no legal infrastructure to regulate commercial transactions online.
3. Corporate will now be able to use digital signatures to carry out their transactions online as legal validity and sanction given under the IT Act, 2000.
4. The IT Act, 2000 also throws open the doors for the entry of corporate in the business of being Certifying Authorities for issuing Digital Signature Certificates. The law does not make any distinction between any legal entity for being appointed as a Certifying Authority so long as the norms stipulated by the IT Act, 2000, rules and regulations made there under have been followed.
5. The Act also enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate government in the electronic form as may be prescribed by the appropriate government, thereby saving costs, time and wastage of precious manpower.
6. Corporate is mandated by different laws of the country, to keep and retain, valuable and corporate information. The IT Act, 2000 enables companies legally to retain the information in the electronic form, if

- the information contained therein remains accessible so as to be usable for a subsequent reference;
- the electronic record is retained in the format in which it was originally generated, sent or received or in a format, which can be demonstrated to represent accurately the information originally generated, sent or received;
- the details, which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record, are available in the electronic record.

7. The IT Act, 2000 addresses important issues of security, which are so critical to the success of electronic transactions. The Act has given legal definition to the concept of secure digital signatures, which would be required to have been passed through a system of a security procedure, as agreed to by the parties concerned. In times to come, secure digital signatures shall play a major role in the New Economy, particularly from the perspective of the corporate sector, as they will enable more secure transactions online.
8. In today's scenario, information is supreme. Information is stored by the companies on their respective computer systems, apart from maintaining a back up. Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy if anyone breaks into their computer systems or networks and causes damages or copies data. The remedy provided by the IT Act, 2000 is in the form of monetary damages, by way of compensation, not exceeding Rs. 100, 00,000. Corporate in India can now heave a sigh of relief as the IT Act, 2000 has defined various cyber crimes and has declared them penal offences punishable with imprisonment and fine. These include hacking and damage to computer source code. Corporate often face hacking in their systems. Prior to the coming into effect of the Indian Cyber law, the corporate were helpless as there was no legal redress for such issues. However, the IT Act, 2000 changes the scene altogether.

Conclusion

The ever-changing nature of the cyberspace necessitates a proactive, global approach to effectively combat cyber-attacks. By leveraging international best practices and promoting cooperation between nations, as well as implementing strong legal frameworks, we can mitigate cyber threats and ensure a safer digital space for all parties involved. Cybercrime exists in almost every country, and the governments are taking steps to protect against it. Since 2020 when the covid-19 pandemic started, everyone, from children to seniors, has been relying on the digital space. As a result, there has been a rise in cybercrime during this time. Cyberbullying, defamation, and cyber fraud have become the most common cybercrime. The reason behind this is the ease of access of devices, and sometimes the negligence of users. In India, most people are unaware of these crimes and when hacked, they lose money but do not know what happened. Therefore, it is very important to know about these crimes and about their rights in the digital space. Even though the Indian government has implemented measures to prevent cybercrime, there is still no end to it.

References

1. Text of the council on Europe's convention on cybercrime treaty, budapest, available at, 2001. https://www.aclu.org/legal-document/text-council-europes-convention-cybercrime-treaty last accessed on 2nd August 2019
2. Henrik WKK aspersen. Cyber Racism and the Council of Europe's reply available at https://www.humanrights.gov.au/our-work/cyber-racism-and-council-europes-reply accessed on 2nd August 2019
3. EU hi-tech crime agency created, 12:55 GMT available at, 2003. http://news.bbc.co.uk/2/hi/technology/3226178.stm last accessed on 2nd August 2019
4. Aaron Scullion. Iran's president defends web control, 10:31 GMT available at, 2003. http://news.bbc.co.uk/2/hi/technology/3312841.stm last accessed on 2nd August 2019