International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Impact of Cybercrime on E-Governance. Is Cybercrime Affecting the Confidentiality of Government Data?

Megha Saxena

Email: *meghasaxena901[at]gmail.com*

Abstract: ***As per the Statistics, Cybercrime was registered and treated at the time of COVID-19 which includes 790 complaints approximately. In the year 2019, the graph of complaints reached 6,67,363 from 70% which resulted to occur a loss of $4.2 billion. The graph of Cybercrimes has been increasing at a high rate all around the globe which has created a huge tension among the countries. The paper will analyze why cybercrime is touching its peak and why the offenders are not able to be caught easily, even though with excessive security and technical knowledge of the officials. Cybercrime in earlier stages was only limited to individuals or groups of individuals but in recent times it is extended to the government of the countries which has created the major tension. As a result, the government has conducted several training and educational programs to guide the officials in tracking the offenders of cybercrime. Several laws prevailed including the Information Technology Act, of 2000, the Indian Penal Code, the Companies Act, and Information Technology Rules, to curb cybercrimes from the country which addition to several International treaties.***

Keywords: Cyber-crime, Covid-19, E-governance, Hacking, Confidential Information, Privacy

1. Introduction

"Cyber Crimes are like a Cancer which had hollowed the people of the society including Government through emotional and financial traumas of heavy financial losses".

At the time of COVID-19, due to the lockdown in almost every country, all the financial transactions were done through online mode which has created the opportunity for the financial criminals to commit various cybercrimes. In the modern era, most of the services are given by the government through online portals and websites and also E-Governance is a new trend that is spreading rapidly around the globe to give several facilities to the citizens of the country as various government and private organizations are considered to secure to be essential to secure the confidential and data but unfortunately increasing cyber-attacks, threats, and crimes have created the insecurity concerning leakage of any information or suffering of huge financial losses. The sensitivity of the situation is rightly mentioned in the report of experts in cybersecurity (CTI) which states that $450 billion is the cost involved in malicious hacking activities and suggests that investigation is a must to capture the international online hacker community. The statistics of the report stated that the total cyberattacks so far were US$6 trillion in the year 2021 and the graph has increased after Covid in so far. The paper will analyze the impacts of cyber security on several areas of society including the medical domain and essentially on the E-Governance with all actions the governments around the globe have taken to reduce the cybercrimes through making of several laws and signing of several international treaties and conducting meetings at the international level with some suggestions for further improvements as the situation arises[1]. The main objective of my study is to examine to what extent cyber laws can combat cybercrime by identifying the inadequacy of laws and what steps could be taken in improvement to curb cybercrimes with suggestions for the solution to the biggest problem of this modern era drawn from several legal international framework and reports.

1.1 Cybercrimes, Cyber Attacks and E-Governance:

Cybercrime is a crime that is done by using a computer or technical gadgets with a network or the internet.They are considered non-violent crimes which are essentially done for financial gains by illegal means and sometimes to cause personal harm to the victim. Most businesses become victims of hacktivists where all the financial and confidential data is being hacked by the hacker which leads to major business losses, similarly, cyberattacks are alike which mostly likely to steal information by damaging the data or the computer programs of one or more computers using various illegal cybercriminal activities. As technology is upgrading and in trend nowadays the chances and parameters of cyberattacks are at boom. The cybercrimes and cyberattacks are mainly affecting e-governance as there is a list of cases coming so far related to cyber-attacks on e-governance. E-governance is the type of modern governance that is considered the use of Information and communication technologies (ICT) to make easy and convenient government operations with recording of online data as a piece of confidential information online with the government which makes it an integral part of the modern era. Unfortunately, cyber crimes have questioned the confidentiality of the data stored by the government and created a sense of insecurity.

[1]The Impact of Cyber Attacks on E-Governance During the COVID-19 Pandemicavailable at: https://www.researchgate.net/publication/360198895_The_Impact_of_Cyber_Attacks_on_E-Governance_During_the_COVID-19_Pandemic (Last Modified March, 2022)

1.2 Historical Background

The origin of cybercrime can be traced roughly 30 years back on the boom the hack in the year 1834 in history is considered to be the first cybercrime where two crooks hacked the French telegram system and committed data theft by getting access to financial markets by illegal means. The next target was telephoned in the 20th century when one boy stole Alexander Graham's telephone and started making misleading calls which became popular in the 1960s and 1980s. Further, the introduction of mail has created phishing schemes where viruses were and are sent through links on emails in addition to email bombing which was further continued and is at boom in the present scenario.

2. Pillars of E-Governance

The E-governance provides services through its four pillars mentioned below:

2.1. **Connection and connectivity:** This pillar act as a connection to connect the people at large which is proven to be essential for effective working of the E-Governance.

2.2. **IT Knowledge:** This pillar acts to employ skillful engineers for its effective working and to handle its day-to-day functioning and if any disruption arises then they may handle it effectively on an urgent basis.

2.3. **Database and Data content:** This pillar acts to provide or share information on different platforms that need a database for e-governance.

2.4. **Capital Required:** This pillar act for the financial issues for the governance to provide services or sector of the economy based on this operation.

3. Services Provided by E-Governance[2]:

3.1. **Government to Citizen (G2G):** These are the types of services where the services are directly provided by the government to the citizens which provides access to the information and services. In this, the citizens can directly ask questions and receive answers from government agencies with the filing of income taxes, renewing of driving licenses, payments of traffic tickets, etc.

3.2. **Government to Business (G2B):** These are the types of services that are directly provided by the government to businesses. In this, the transactions can be from government to business or business to government which deals with several departments including the transport department, labour department, tourist association, registration department, social welfare department, etc.

3.3. **Government to Government (G2G):** These are the types of services that function when two government agencies or organizations function together on an activity. For eg: The federal case registry which dealt with child support, Interlink which dealt with some classified information by various US intelligence agencies, etc.

3.4. **Government to Constituents (G2C):** These are the types of services that deal with online activities conducted by the government including democratic procedures, current affairs discussion, etc.

4. Types of Cybercrimes in E-Governance[3]:

4.1. **External Cyber Crimes:** These are the type of attacks which is done by groups of cyber criminals to cause financial damage to large companies and organizations in return for pay, blackmail, extortion, etc. They are mostly accomplished by the computers by breaking poor security codes of the government.

4.2. **Internal Cyber Crimes:** These are a type of Cybercrimes which is conducted by the employee of the organization where he steals confidential data and information and leaks with the foreign power or competition of the organization in return for huge amounts of money.

4.3. **Malicious Software Cybercrime:** These types of Cybercrimes include Viruses that cause full damage to the computer system, Trojan horse that seems normal but generate a malicious program in the computer system, and back doors that are set up by the cybercriminals to gain access into the computer system.

4.4. **Web Hacking:** This type of cybercrime hacks the websites of the government and organizations using web hacking to deface their reputation by showing weak security.

4.5. **Cyber Espionage:** This cybercrime commits a crime by stealing the confidential and sensitive information of the organization.

5. Social and Legal Impact of Cyber Crime on Confidentiality of E-Governance:

5.1 Diminished Trust: An increase in cybercrimes at government systems results in increased insecurity among the people to use government services as they have a fear of leaking confidential and sensitive data.

5.2 Disruption in Government services: This cybercrime in E-Governance affects the accessibility of the citizens to use the required and important information or to complete any important transaction.

5.3 Financial Repercussions: To investigate, mitigate, and recover from cybercrimes and cyberattacks they huge amount of money is required in addition to it several

[2] Impact of Cyber Security in Different Application of E-Governance, India, available at: https://ignited.in/a/57309 (Last Modified June, 2018)

[3] Types of Cybercrime, India, available at: https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/ (Last Moified March 22, 2023)

charges of compensation to the person affected and legal liabilities are involved.

5.4 Threat to National Security: In cybercrimes, cybercriminals hack sensitive confidential information with defense systems and classified infrastructure which could be a huge danger to the nation.

5.5 Theft of Intellectual Property: In cybercrimes, cybercriminals can steal information related to a nation's Intellectual property and leak it which can harm the national security of the country.

6. Cyber Security in E-Governance

Whenever cybercrimes and cyberattacks are at boom then cybersecurity is the tool that can curb the problem and save the country, citizens of the country, and the government. Cybersecurity helps to control access to networks and secure information. It can be performed on a reliable and trustworthy platform that is digital in nature. In most cases wherever cyberspace is weak, incomplete, absent, or not designed property leads to an increase in the chances of cyberattacks.

The cyber-security is the combination of 3 objectives which are:

- Prevent, detect, and respond
- People, processes, and technology
- Confidentiality, integrity, and availability.

This covers various types of processes and controls that play an essential role in the successful implementation of an information security policy experienced by leading technological countries.

7. Cybercrime Laws in India

7.1 Information Technology Act, 2000

As the rate of cybercrimes in India was booming there was a need for a separate which only deals with offences related to cyber. The IT Act was the first act on cybercrimes that was approved by the parliament to provide the legal recognition of all the transactions that are done through electronic data exchange which in other words referred to as the electronic methods of communication and storage of information. In addition, it has also amended the Indian Evidence Act, of 1972, the Banker's Book Evidence Act, the Reserve Bank of India Act, of 1934, and the Indian Penal Act, of 1860.

Section 43: Given section of the IT act applied to those cybercriminals who have damaged the computer of the other person referred to as victim without permission will be liable for the compensation of the damage

Section 66: This section describes the punishment that will be granted to the offender who has committed the offense under Section 43 of the act is up to 3 years of the punishment and a fine extending up to 5 lakhs.

Section 66B: Given section describes receiving any stolen communication devices or computers fraudulently will have to face imprisonment for up to 3 years and a fine can extend up to 1 lakh.

Section 66C: The given section describes the cybercriminals committing Identity theft by password hacking or fake digital signatures have to face imprisonment of up to 3 years and a fine of up to 1 lakh.

Section 66E: The given section describes the offense of taking private pictures and publishing them without the consent of the person will be punishable for up to 3 years or a fine of up to 2 lakhs.

Section 66F: The given section describes the cybercrimes related to cyberterrorism.

Section 67: The given section describes that publishing obscenities electronically will be punishable for up to 5 years and a fine of up to 10 lakhs.

7.2 Indian Penal Code,1860

Section 292: The given section describes the cybercrime related to the sale of obscene materials. All the acts of the cybercriminals related to publishing obscene and sexually explicit acts of the children come in the ambit of this section and severely punishable imprisonment up to 2 years and a fine of 2000/- and for the repeated offender imprisonment of up to 5 years and a fine up to 5000/-

Section 354C: The given section describes publishing pictures or recording of any video which involves no consent of the woman e.g.: pictures of her private parts. This section is wide enough to involve voyeurism which involves watching a woman's sexual acts of which she has not consented.

Section 379: This section describes hacked and hijacked electronic devices with stolen data or stolen computers will be punishable for up to 3 years in addition to the fine.

Section 420: This section describes cyber fraud, the creation of fake websites, and the delivery of property using cheating and dishonest intentions will be punished with imprisonment of up to 7 years and an additional fine.

Section 465: This section describes about the offense of forgery which is punishable under this act by imprisonment for up to 2 years.

7.3 Companies Act, 2013

The Companies Act, 2013 was made to properly manage the daily operations of the company and its legal obligations. The SFIO which means Serious Fraud Investigation Office is a part of the Companies Act and has the power to investigate and prosecute serious crimes like frauds committed by Indian directors and Indian companies.

8. International Cybercrime Laws

8.1 The United States of America: The cybercrime law in the USA is the 'Fraud and Abuse Act' which prohibits computer fraud and abuse and also protects federal banks and internet connections from any kind of threat, vandalism fraud, etc from national and international cybercriminals.

8.2 Canada: 'The Criminal Code of Canada' in collaboration with the Personal Information Protection and Electronic Documents Act is made to curb the cybercrimes in Canada which act as a data privacy act and put two key cybersecurity duties on Canadian private sector organizations.

8.3 European Union: There are several laws but the most comprehensive and unified cyber law is the 'General Data Protection Regulation Act'. This law applies to all the corporations working in the EU and a special impact is on foreign corporations doing business in the EU which was established in 2018. This act imposes penalties and fines with payment of compensation by the cybercriminal to the victim of the cybercrime.

8.4 China: The cyber law in China is "Data security law" whose primary objective is to safeguard and provide security to all the important and confidential data of the government which is essential in the public interest and which is essentially related to national security.

8.5 United Kingdom: The cyber law prevails in 'The United Kingdom is Computer Misuse Act,2013' which imposes criminal penalties on offenders who traffic technology for unauthorized computer access.

9. Budapest Convention on Cyber Crime[4]

The Budapest Convention is the first and foremost International treaty where the crime related to computers and the internet has been addressed by the corporation of the nations and harmonizing the several national laws to improve the investigative techniques. This convention was proposed by the Council of Europe in Strasbourg, France.

It has also included observant states including Canada, Japan, the Philippines, South Africa, and the United States.

The final report with the Explanatory report was adopted in the 109th session in addition to some other problems that need to be discussed including racism and Xenophobia.

Other international treaties related to cybercrimes

- United Nations of Convention Against Transnational Organized Crime (2000)
- Convention on Cybercrime (2001)
- Optional Protocol to the Convention on the Rights of the Child (2001)
- Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems (2003)[5]
- Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (2022)
- Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007).

10. Cases Related to Cybercrimes

10.1 Kumar v. Whiteley[6]

Facts: In this case, the accused gained access to JANET which is (a joint academic network) with fraudulent intentions moreover he deleted, added, and changed the file data files also being an unauthorized user he had to log in to BSNL broadband connection.

Held: The CBI has registered the crime and found that the accused has committed the cybercrime due to which the victim has suffered a loss of Rs. 38,248. The magistrate had charged him for a rigorous punishment of a year and a fine of 5,000/-

10.2 Shreya Singhal v. Union of India

Facts: In this, the two women had posted offensive and objectionable comments after the demise of a political leader because of which they were arrested u/s 66A of the IT act. They defended by saying that this arrest was a total violation of their Freedom of speech and expression.

Held: The Supreme Court held that all the fundamental rights have their reasonable restrictions concerning public peace and harmony similarly any speech or expression that can disturb the public order, security, health, etc will not be considered a Fundamental right.

10.3 Shankar v. State Rep

Facts: In this case, the petitioner had gained unauthorized access to the confidential and protected system of the Legal advisor of the Directorate of Vigilance and Anti-corruption (DVAC) to quash the charge sheet filed against him. The petitioner was charged u/s 66,70 and 72 of the IT Act.

Held: The Court noted that, in light of the legislation on the denial of prosecution sanction under Section 72 of the IT Act, the charge sheet brought against the petitioner cannot be revoked.

11. Conclusion

[4]The Budapest Convention (ETS No. 185) and its Protocols, available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Last Modified October 23, 2023)

[55]International and Foreign Cyberspace Law Research Guide, available at: https://guides.ll.georgetown.edu/cyberspace/cyber-crime-treaties (Last Modified October 23, 2023)

[6]Important Cyber Law Case Studies, available at: https://www.cyberralegalservices.com/detail-casestudies.php(Last Modified October 23, 2023)

E-governance has become a revolutionary force in the quickly changing digital era, offering efficiency, openness, and accessibility in the provision of public services. Although there are many advantages to digitizing government procedures, governments are now more vulnerable to the persistent danger of cybercrime. The various ways that cybercrime affects e-governance and the privacy of government data have been examined in this article, underscoring the pressing need for strong cybersecurity defenses and proactive efforts to protect sensitive data.

Cybercrime has penetrated the core of e-governance systems with its wide range of tactics and incentives. These attacks have far-reaching consequences since they jeopardize the integrity of public services and threaten the basic foundations of democratic institutions. The most notable effect is the decline in public confidence in the government. Citizens are reluctant to interact with e-governance platforms when they believe that government data is not secure or secret. Consequently, this undermines the goals of e-governance as it does not fully utilize digital technology to include residents and provide effective services.

To sum up, cybercrime presents a serious threat to government data confidentiality and e-governance. Its effects are seen well beyond the digital sphere, as it undermines public service integrity, damages citizens' faith in their governments, and costs money. Governments may, however, strengthen their e-governance systems and preserve the privacy of public data by taking a proactive approach to cybersecurity, collaborating internationally, and dedicating themselves to data protection. It is our joint duty to see to it that the promises of e-government are kept, offering citizens effective, safe, and transparent services while respecting the fundamentals of democracy and sound administration.