LEX SCRIPTA MAGAZINE OF LAW AND POLICY

ISSN- 2583-8725

VOLUME-1 ISSUE-1
YEAR: 2023

EDITED BY:

LEX SCRIPTA MAGAZINE OF LAW AND POLICY

LEX SCRIPTA MAGAZINE OF LAW AND POLICY, VOLUME-1: ISSUE-2

LEX SCRIPTA MAGAZINE OF LAW AND POLICY, VOL-1, ISSUE-1
ISSN-2583-8725

INFLUENCE OF CYBER LAWS ON DATA SECURITY: AN ANALYSIS

AUTHOR: KUMAR ARYAN

ABSTRACT

The internet has now become an integral part of everybody' s daily routine. Everything in the world is affected by it, from online purchasing to simple conversations. Businesses have also opted to do their business online; E-commerce has thus become more well-known. Nowadays, a lot of official business is done online, and e-finance has become quite popular in the past year. The risks associated with using the internet have increased as its use has grown. Thus, everything is stored online in the form of data. In this era of online data storage, data protection becomes a necessary provision. Data security or data protection is screening of data from any unauthorized access throughout its lifecycle. To tackle data threat provisions under the Indian laws have been made. Cyber laws deal with safeguarding data and prescribe punishment related to data theft and other similar activities.

The paper deals with the influence of cyber laws on data protection in India along with legal aspects.

Keywords: internet, data, data protection, data security, cyber laws.

INTRODUCTION

To safeguard their vital assets, businesses all over the world are making significant investments in information technology (IT) cyber security capabilities. The methods for incident detection and response to protecting organizational interests have three common elements: people, processes, and technology. This is true regardless of whether an enterprise needs to protect a brand, intellectual capital, and customer information or provide controls for critical infrastructure. Cyberattacks, information misuse, and data sharing are all considered forms of cybercrime since data and information are now considered assets of all enterprises. As a result, measures have been implemented to combat this crime in many parts of the world. The nations that accept acts need to enhance it by embracing technology and educating their citizens and organisations. On the other side, the nations where no such crimes have occurred are the most susceptible in this situation, therefore they must adopt the best practices from other nations and establish an exhaustive law for their areas to outlaw this kind of crime and punish those who do it.

The Information Technology Act 2000 (the IT Act) and a number of other acts serve as a standin for data protection legislation in India as there is not any special legislation for this matter. According to a 2017 decision by the Indian Supreme Court, people of India have a basic right to privacy that is principally protected by Article 21 of the Indian Constitution. According to the Court, this right encompasses, among other things, the right to informational privacy. In the wake of this ruling, a 10-member committee headed by former Supreme Court Judge BN Sri Krishna was appointed in order to give it substance through comprehensive legislation. The Sri Krishna Committee released a report that looked at the patchwork of pertinent laws that exist in India today, researched other countries' statutory approaches to privacy and data protection, and provided a thorough justification for a better legal system. A proposal of the 2018 Personal Data Protection Bill was included with the study.[1]

[1] *Aditi Subramaniam, Sanju Das, (2022, October 27) The Privacy, Data Protection and Cybersecurity Law Review: India, The Law Reviews. https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecuritylaw-review/india*

CYBER LAW AND IT's IMPORTANCE

The term ‗cyberlaw' consists of two words, ‗cyber' and ‗law.' The word ‗cyber' means anything related to information technology as to compute on the internet, and the word ‗law' means any set of procedural rules and regulations which has been entrenched in society to follow to ensure peace and harmony. Thus, cyber laws are such procedural rules and regulations that regulate technological threats, where a computer or any similar device is used either as a target or as a tool. It includes regulations for accessing and using the internet and even lays out guidelines for preserving online privacy. Cyber law covers a wide range of concerns, including legal informatics and electronic components like computers, software, and hardware, as well as information systems. It is the legal framework that must be used to combat cybercrimes.

In short, cyber law refers to the body of rules and regulations governing the use of the internet and other forms of networking and information technology in accordance with norms of law, justice, and ethics. It is relevant to the internet and associated technologies.[2]

CATEGORIES OF CYBER CRIME

Cybercrimes are broadly classified into three:

iv. Crime Against Individuals

Cyber-crimes against specific people include cyberdefamation, hacking, indecent exposure, spoofing emails, IRC crime (Internet Relay Chat), net extortion, malicious code, trafficking, distribution, posting, phishing, credit card fraud, and the spread of pornographic material, including software piracy. There is perhaps no crime that could do an individual more harm. **v. Crime Against Property**

theft of any kind of property. These offences include computer vandalism (erasing other people's property), salami attacks, and intellectual property violations. This kind of crime is commonly perpetrated in or with the aim to commit financial crimes at financial institutions. The adjustment being so little that it usually goes unreported is a vital aspect of this type of offence.

vi. Crime Against Organization

One specific type is cyberterrorism. The advancement of the internet has shown how individuals and organizations are using the standard of cyberspace to intimidate national and international governments as well as to terrorize their citizens. When a person cracks into a website that is administered by the government or the military, this offence clearly becomes terrorism. [3]

ABOUT DATA PROTECTION AND DATA PRIVACY

Data can take on any form, including computer printouts, magnetic or optical storage media, punched cards, punched tapes, or being stored internally in the memory of the computer. Data is defined as a representation of information, knowledge, facts, concepts, or instructions which are being prepared or have been prepared in a formalized manner, and are intended to be processed, is being processed, or has been processed in a computer system or computer network.

---

[2] *Analysis of cyber law in India, Prime Legal. https://primelegal.in/2022/10/15/analysis-of-cyber-law-in-india/*

[3] *Bandakkanavar, R. (2022, June 27).Causes of CyberCrime and Preventive Measures Krazytech. https://krazytech.com/technical-papers/cyber-crime*

Accumulation of facts in the form of numbers, measurements, observations or passwords, anything that can be fed into a computer system is data. Data can be personal data, the information which is related to a person specific and is used for identification of the particular person. Any specifications such as name, address, phone number, pan card or any other such card number, even the medical reports or IP address of the device which is used by the person are considered as personal data.

Thus, to safeguard data, data protection is required. Data protection is the synchronization of techniques and practices used to secure the confidentiality, usability, and integrity of the data. This synchronization prevents any potential of data loss, theft, or corruption, and should a breach occur, it may assist to mitigate the harm done.

Data protection and Data privacy are interconnected to each other.

The concept of data privacy is more akin to dictating how data should be gathered and managed based on how sensitive and important the data is that is being supplied. The rules governing data protection are used to manage data privacy. Although data protection safeguards the data from those who do not have access to it, data privacy specifies who has access to the data.

Every level, whether personal, business, or governmental, protects data; however, the method and scope used at each level might vary depending on the circumstances, including who requires access and whose data has to be protected. A few perspectives must be kept in mind during the data protection procedure. The procedure, regardless of the degree at which it is being carried out, must stay within a certain range; anything in excess is harmful, and the data must be accurate and pertinent in nature.

The most important justification for data protection is that it protects all forms of valuable data and prevents unauthorized access to it by anybody. It also aids in maintaining a line of privacy, as when an employee gives personal information to the HR department of a company, which keeps the information to itself and forbids any unauthorized access, or when a client shares the information. When this line of privacy is maintained, it increases the trust and confidence of clients in the organization, which in turn aids the organization's survival in society.

LAWS FOR DATA PROTECTION IN INDIA

Specific Act for data protection has not been enforced in India. However, laws for data protection and privacy have been deduced from existing following statutes.

i. Constitution of India

Although there is no specific provision for Right to Privacy, the courts have derived it from existing provisions in relation to fundamental rights. As stated under Article 21 ―No person shall be deprived of his life or liberty except according to the procedure established by law‖. Right to Privacy takes its frame from Article 21. In the case of **M. P. Sharma and Others. V Satish Chandra, District Magistrate, Delhi, and Ors.**[105], the Supreme Court refrained from acknowledging the right to privacy as a part of Article 21. The question whether Right to Privacy is a part of Article 21 was first answered in the landmark case of **Maneka Gandhi v Union of India.** The apex court held that Right to Privacy was a vital component of right of life under Article 21 of the Indian constitution.

ii. Indian Contract Act, 1872

S. 27 of the said Act provides that a person would be compensated in case of data leakage of any manner and also lays down the mechanism to be imposed with the person who is behind such data leakage depending upon to what extent it is leaked.

iii. Indian Penal Code, 1860

The said Act was amended to include the term "data" in the definition of "movable property," making data theft or its misuse a violation of the act. Because they are mobile by nature, computer data or databases are protected under the legislation. It has been demonstrated to be extremely successful in preventing data theft.

iv. Copyright Act, 1957

This act provides protection to the Intellectual Property Rights of all kinds of works including the literary, dramatical, artistic work. The word "literary work" now includes computer databases owing to an amendment to the legislation. Customers will profit from the modification as no other institution, save the service provider, is permitted by law to utilize the information they submit in any way.

v. Information Technology Act, 2000

This law was established as a foundation for managing the virtual economy, which includes ecommerce, electronic contracts, emails, and much more. The statute was passed in 2000, but since then, the virtual environment has expanded greatly, making it increasingly relevant in nature. It grants all transactions aided by the electronic technique, commonly referred to as ecommerce, a legal standing.[106]

[105] *1954 AIR 300, 1954 SCR 1077*

[106] *Analysis of cyber law in India, Prime Legal. https://primelegal.in/2022/10/15/analysis-of-cyber-law-in-india/*

vi. The Personal Data Protection Bill, 2006

The Personal Data Protection Bill, now under consideration as data protection legislation in India, was inspired by the ruling in **K. S. Puttaswamy (Retd.) v. Union of India[4].** Although Parliament has not yet approved it, it provides us with a good indication of the development of India's data protection regulations. In July 2017, the Ministry of Electronics and Information Technology appointed a committee headed by former Supreme Court Judge B. N. Sri Krishna to investigate issues with data privacy.

CONCLUSION

Data will increase in value day by day due to the exponential rise in the number of individuals producing and consuming it globally. It will be crucial to protect citizen data since data drives growth. Governments from all over the world will need to modify existing laws or create new ones in order to keep up with the continuously evolving nature of technology. Due to the internet's integration into daily life, both legal and illegal acts have been done on computers and other digital sources on a large scale. The government must adjust by enacting new laws that consider the reality of the digital era as cybercrime frequency rises. Cyber law establishes what is permitted and prohibited online.

Although consumers freely divulge personal information when making purchases online or exchanging emails, it is the duty of the State to monitor and safeguard the interests of its citizens.

A set of laws and guidelines specified in the Information Technology Act of 2000 control cybercrime. The battle against crimes that target computer systems and networks also depends on this law. People

[4] *No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 416*

may easily conduct safe online financial transactions inside the legal system thanks to cyber law. In other words, the legislation has made it easier for us to utilize all technological gadgets.