CYBERLAW: A REQUISITE IN THE MODERN ERA

Dhruv Jadaun*

ABSTRACT

Cyber-law awareness is the knowledge of the legal principles governing conduct and behavior online. Cyberlaw is more important than ever thanks to the internet's explosive growth and the rising use of digital gadgets. It covers a wide range of topics, such as online defamation, data privacy, intellectual property rights, and cybercrime. Individuals, companies, and organizations must be aware of Cyberlaw to follow the law and protect themselves from liability. It aids individuals in comprehending the legal ramifications of their online actions and conducts as well as how to defend their rights and interests in the digital sphere. Also, it makes it possible for law enforcement authorities to efficiently look into and prosecute cybercrime. Even though Cyberlaw is becoming increasingly significant, many people and businesses are still unaware of it. Legal issues including data breaches, identity theft, and internet abuse may result from this ignorance. Thus, it is crucial to raise an understanding of Cyberlaw through programs of instruction, training, and public outreach.

Keywords:-Cyber-law, Cyber-crime.

INTRODUCTION

Cyberlaw, commonly referred to as Internet law or digital law, is the body of legislation that governs how people utilize the Internet and electronic gadgets. Cyberlaw has taken on more significance in contemporary society as a result of the internet's and technology's fast development. Data privacy, cyber-security, e-commerce, intellectual property, and cybercrime are just a few of the legal concerns it covers.[1]

Cyberlaw's main goal is to safeguard people and businesses from the dangers connected to using the internet and electronic gadgets.[2] It attempts to protect individual rights and freedoms while ensuring that online actions and behaviors are carried out legally and morally. Online auctions are governed by civil and criminal rules together known as Cyberlaw. It encompasses a wide range of legal disciplines, including criminal law, contract law, tort law,

*BA LLB, FIRST YEAR, INSTITUTE OF LEGAL STUDIES AND RESEARCH, GLA UNIVERSITY, MATHURA.

[1] LAWSHELF, https://lawshelf.com/videocoursesmoduleview/introduction-to-cyberlaw--module-1-of-5 (last visited Feb. 5, 2023).

[2] *Ibid.*

and intellectual property law. Cyber-law, for instance, may be used to prosecute online criminals including hackers, online con artists, and cyberbullies.

CYBERCRIMES CAN BE ENCIRCLED RELATED TO

Depending on the sort of crime, there are many categories into which cyber crimes can be divided. Following are a few typical types of cyber-crimes:

Cyber fraud: This includes any illicit online behaviour, including phishing schemes, online fraud, and identity theft.

Hacking: To steal data, interfere with operations, or otherwise do harm, this refers to illegal access to computer systems or networks.[3]

Malware: This particular kind of malware is intended to harm or take down computer systems, steal information, or grant unauthorized access to them.

Cyberstalking: This is when someone is threatened or harassed through electronic communication, most frequently through social media, email, or text messaging.

Cyberbullying: This is the practice of intimidating or harassing someone online, frequently through social media, chat rooms, or SMS messages.

Cyberterrorism: This is using technology such as computers to carry out terrorist activities, such as breaking into vital infrastructure systems or conducting a cyberattack against a company or government.

Cyber espionage: This occurs when a government or organisation is targeted to steal sensitive data or trade secrets.

Copyright infringement: This comprises the illegal use of intellectual property, including software, movies, and music, which may be accomplished through file sharing or internet piracy.[4]

Cyberwarfare: This is the use of computer technology, frequently in the context of military action, to interfere with or destroy an adversary's computer systems.

[3]NORWICH PRO, https://pro.norwich.edu/academic-programs/resources/types-of-cyber-crime (last visited Feb. 7, 2023).
[4]CUTEO LAW GROUP, https://cuetolawgroup.com/types-of-cybercrime/ (last visited Feb. 7, 2023).

OBJECTIVE OF CBER LAW

Cybercrime prevention for individuals and organizations: Digital Regulation expects to safeguard people and associations from different cyber-crimes, for example, hacking, phishing, fraud, cyber-bullying, cybers-talking, and cyber-terrorism. It aids in the prevention of such activities and provides victims with legal recourse.

Regulating behaviour online: By establishing guidelines and guidelines for online behaviour, Cyberlaw regulates online behaviour. It helps to stop online abuse, cyberbullying, and other types of bad behaviour.

Intellectual property protection: Individuals' and organizations' intellectual property rights in cyberspace are safeguarded by Cyberlaw. Copyrights, trademarks, patents, and other forms of intellectual property are safeguarded by it.

Promoting online shopping: By providing a legal framework for online transactions, Cyberlaw encourages e-commerce. It contributes to the assurance that online transactions are legal, authentic, and secure.

Securing and protecting data: By establishing standards and guidelines for the collection, storage, processing, and sharing of personal and sensitive information in cyberspace, Cyberlaw ensures data privacy and security.

International cooperation facilitation: By providing nations with a unified legal framework within which to collaborate in the fight against cybercrime and other cyber-related issues, Cyberlaw facilitates international cooperation.

Promoting awareness of cyber-security: The goal of Cyberlaw is to educate individuals, businesses, and governments about cyber-security. It teaches people about the dangers of using the internet and shows them how to defend themselves against cyberattacks.

HISTORY OR ORIGIN OF CYBERLAWS[5]

Cyberlaws are a body of rules that control how the internet and other digital technologies are used. They are often referred to as internet laws or digital laws. As the potential for online crimes and abuses first emerged in the early years of the internet, Cyberlaws were created. The United States Computer Fraud and Misuse Act (CFAA), which has been passed in 1986, was the first significant piece of cyber-law legislation. A wide range of computer-related

[5]LEGAL SERVICE INDIA, https://www.legalserviceindia.com/(last visited 9 Feb. 2023).

offences, including hacking, virus attacks, and cyber-stalking, are now included under the CFAA, which originally made it unlawful to enter a computer without authorization.

The Data Protection Directive, which established a framework for the protection of personal data in the EU, was passed by the European Union (EU) in 1991. Later, in 2018, the General Data Protection Regulation (GDPR), which tightened individual privacy rights and set stiffer penalties for non-compliance, superseded the directive. With the creation of the UN Commission on International Trade Law (UNCITRAL) in 1966, the UN also contributed to the creation of Cyberlaws. Since then, UNCITRAL has contributed to the creation of international treaties and model legislation about electronic commerce, digital signatures, and online dispute resolution. Cyberlaws have advanced and complicated along with the internet. In the modern world, there are several Cyberlaws and regulations in force that cover everything from online privacy and data protection to cybercrime and intellectual property rights.

THE CYBER-LAWS AND THEIR PUNISHMENT

The penalty for breaking Cyberlaws, which govern internet and computer use, might differ depending on how seriously the act was committed. Following are a few instances of Cyberlaws and their associated penalties:

Cybercrime law: This legislation makes a variety of behaviours unlawful, including identity fraud, spam, hacking, and cyberbullying. Depending on how serious the offence was, these offences may result in fines, jail, or both.

Data protection laws: These rules govern how personal data is gathered, used, and shared online. Depending on how serious the violation was, breaching this statute might result in fines, jail, or both.

Intellectual property law: This regulation protects against the unlawful use and distribution of digital assets, including music, videos, and applications. Depending on the seriousness of the act, the penalty for breaking this legislation may consist of fines, imprisonment, or even both.

Cyber-stalking Law: This legislation forbids harassing or intimidating someone online or by other technological methods. Depending on how serious the violation was, breaching this statute might result in fines, jail, or both.

Cyber-terrorism Law: This legislation makes it illegal to carry out terrorist activities using electronic devices. Depending on how serious the violation was, breaching this statute might result in fines, jail, or both.

PROBLEMS OF CYBERLAW

Cyberlaw, which deals with legal concerns relating to the use of the internet and technology, is a relatively young field of law. Cyberlaw is becoming more crucial as technology develops and permeates our daily lives more and more. Among the issues with Cyberlaw are:[6]

Legal Issues: Because the internet is a worldwide network, it's possible that the laws of one nation may not apply to another. When it comes to pursuing cybercrime or upholding intellectual property rights, this may give rise to jurisdictional problems.

Absence of International Laws: There is presently no international Cyberlaw, and each nation has its own set of rules and laws. When it comes to applying rules across international borders, this may lead to ambiguity and uncertainty.

Cybercrime: Due to jurisdictional concerns and the anonymous nature of the internet, cybercrime is a developing problem. It can be challenging to prosecute cyber-criminals. Online fraud, identity theft, and hacking are examples of this type of crime.

Privacy Concerns: Privacy concerns are essential because of the rise in the sharing of personal information online. The right to be forgotten, surveillance, and data protection are all included in this.

Problems with Intellectual Property: Intellectual property issues have increased as a result of the ease with which copyrighted content can be shared and distributed thanks to the internet. Trade secrets, trademark infringement, and copyright violations are all examples of this.

Cyberbullying and Internet Harassment: Because of the anonymity of the internet, victims of cyberbullying and online harassment may suffer severe repercussions.

Problems with Free Speech: The internet has developed into a forum for free expression, yet there are worries about online harassment, cyber-stalking, and hate speech. It might be difficult to strike a balance between the need to safeguard people from danger and their right

[6] JAVA T POINT https://www.javatpoint.com/what-is-cyber-law#:~:text=Cyber%20laws%20address%20and%20deal,to%20protect%20a%20person's%20reputation.&text=Harassment%20is%20a%20big%20issue,these%20kinds%20of%20despicable%20crimes(last visited Feb. 10, 2023).

to free expression. In general, Cyberlaw issues are complicated and need an all-encompassing strategy to solve them.

NEED FOR CYBERLAW

Cyberlaw, which deals with concerns relating to the internet, computer systems, networks, and digital data, is a relatively young and quickly developing area of law. Although the demands of Cyberlaw are continually changing, some of the most important ones are as follows:

Protection of personal information: As technology and the internet are used more often, there is a growing need to secure personal information. Personal data can be protected from abuse and unlawful access thanks to cyber legislation.

Cybercrime prevention: A developing issue, cybercrime encompasses hacking, identity theft, and cyber-stalking. Cybercrime prevention and prosecution are made possible by the legal framework of Cyberlaw.

Protection of intellectual property: The development of digital technology has made it simpler to duplicate and share protected content. Intellectual property, including copyrights, patents, and trademarks, is legally protected under Cyberlaw.[7]

Regulation of e-commerce: Cyberlaw offers the legal foundation for doing business online, including contracts, electronic signatures, and online transactions. This regulates e-commerce.

Cyber-security: Protecting computer systems and networks against unwanted access, theft, and destruction is essential in the digital era. Cyberlaw offers the legal basis for doing so.

Privacy protection: Cyberlaw offers legal safeguards for online privacy protection, such as limiting the gathering and use of personal data.[8]

Ultimately, as technology develops, there is a broad and ever-changing demand for Cyberlaw. The safety and security of people and organizations in the digital era depend on cyber legislation.

[7] MEDIUM, https://medium.com/@rohasnagpal/what-is-cyber-law-and-why-do-we-need-it-9e9a9b956b1a(last visited Feb. 12, 2023).
[8] MEDIUM, https://medium.com/@rohasnagpal/what-is-cyber-law-and-why-do-we-need-it-9e9a9b956b1a(last visited Feb. 12, 2023).

INDIAN CYBERLAW

The Information Technology Act of 2000[9]is the principal law in India addressing cybercrime and electronic trade (ITA-2000). The Indian Parliament passed the ITA-2000 Act, which was announced on October 17, 2000.[10] It covers the entirety of India and is made up of 94 parts, 13 chapters, and 4 schedules. The ITA-2000 offers a framework to allow e-filing and e-commerce transactions as well as legal recognition for electronic documents. Moreover, it offers a legal framework for reducing and preventing cybercrimes. The ITA-2000 is administered by the Indian Computer Emergency Response Team (CERT-In) to direct Indian cybersecurity laws, implement data protection rules, and regulate cybercrime.

Examples of supplementary or subordinate laws to the ITA-2000 include the Information Systems (Intermediary Guidelines and Digital Media Ethics Code) Regulations, 2021[11], and the Intermediary Guidelines Rules, 2011. To control online gambling and incorrect or misleading material, the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Regulations, 2023[12], have just been released.

One of the primary issues with India's cyber-security rules is that the government continues to bring cases under unclear or antiquated statutes, which can impede development and the adoption of effective Cyber laws and regulations.[13] The Indian Criminal Code contains provisions that address the majority of criminal laws, including those that may apply to cyber offences in the areas of theft, fraud, identity theft, and intentional infliction of harm. A non-obstante clause, however, in the ITA-2000 states that its provisions take precedence over any other laws that conflict with them. With the creation of the ITA-2000 in 2000, no Indian businesses have faced penalties for data breaches as of August 2022.

SOME CASE LAWS RELATED TO INDIAN CYBER LAW

Some important instances involving Indian Cyberlaw have significantly advanced the system's development. Here are some examples of these situations:

[9]The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[10] INFOSECAWARENESS, https://infosecawareness.in/cyber-laws-of-india(last visited Feb. 15, 2023).
[11]The Information Systems (Intermediary Guidelines and Digital Media Ethics Code) Regulations, 2021, Acts of Parliament, 2021 (India).
[12]*ibid.*
[13]ICLG, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india(last visited Feb. 22, 2023).

Shreya Singhal v. Union of India[14]

An important case involving the constitutional rights to free speech and expression on the Internet was Shreya Singhal v. Union of India. On March 24, 2015, the Supreme Court of India rendered a decision on the matter.

Section 66A of the Information Technology Act, 2000[15], which provides for the punishment of "offensive" and "menacing" online speech, was challenged constitutionally, giving rise to the case. Shreya Singhal, the petitioner, claimed that the clause was ambiguous, overbroad, and in violation of the Indian Constitution's protection of the freedom of speech and expression.[16]

Singhal was right, and the Supreme Court of India declared Section 66A to be unconstitutional. The Court determined that the clause was unconstitutionally broad and ambiguous and that it had a chilling impact on online free expression. The Court stressed the need to defend free expression, especially in the digital era, and concluded that any restrictions on communication had to be specifically tailored to further an important public purpose.

The Singhal case has received a lot of acclaim as a triumph for online freedom of speech and expression in India. Moreover, it has been considered a crucial precedent in other governments attempting to control internet expression.

- **Google India Pvt. Ltd. v. Visaka Industries**[17]

A significant case in Indian law, Google India Pvt. Ltd. v. Visaka Industries, addressed the topics of intermediary responsibility and internet defamation.

In this instance, Visaka Industries sued Google India for posting libellous material on its Blogspot blogging site. The libellous information claimed that Visaka Industries produced and distributed asbestos-containing goods, posing substantial health risks. As Google India did not take down the offensive material despite receiving a complaint, Visaka Industries claimed that Google India was to blame for the defamatory materials.

The court ruled that unless an intermediary, like Google India, had real knowledge of the illegal information and neglected to remove it promptly after receiving a complaint, it could

[14] Shreya Singhal vs Union Of India, AIR 2015 SC 1523.
[15] The Information Technology Act, 2000, § 66-A, No. 21, Acts of Parliament, 2000 (India).
[16] Shreya Singhal v. Union Of India AIR 2015 SC 1523
[17] Google India Private Limited vs M/S Visaka Industries AIR 2020 SC 350.

not be held responsible for the content created by third parties. The court noted that Google India had provided a forum for users to express their thoughts in good faith and that it was unreasonable to expect Google India to manually review all user-posted information.

The court found that an intermediary, such as Google India, could not be held liable for content published by third parties unless the intermediary had actual knowledge of the unlawful information and failed to swiftly delete it after receiving a complaint.[18] The court stated that it was unrealistic to expect Google India to manually evaluate all user-posted content because Google India has offered a place for people to express their opinions in good faith.

SUGGESTIONS

According to the concerns, the government and the legal system must take appropriate action and establish solid legislation that specifies that anybody engaging in criminal activities online will be subject to stringent regulations and punishment.

Due to the surge in cybercrime, the court should enact regulations that are more effective than those they previously created (internet).

Because of the internet and networking in the modern day, where more global online transactions occur, the number of cyber-criminals should be curbed.

The rules and regulations governing cybercrime, as well as the penalties for committing the crime, should be clearly stated on all websites and social media platforms. If someone is engaging in criminal behaviour while being aware of the laws and regulations, they should be held accountable. Even after that, if the offender continues to do so, he will be subjected to servile punishment and also be required to pay a specific sum of money to the court.

CONCLUSION

The phrase "Cyberlaw" refers to a body of guidelines that control actions taken in connection with the internet and other digital communication technologies. Given how technology continues to change the way we live, work, and communicate, it is a crucial component of contemporary civilization. Data privacy, online security, intellectual property, e-commerce, and online defamation are just a few of the many topics covered by Cyberlaw. Cyberlaw will become ever more important as technology develops to safeguard people, organizations, and

[18] BQPRIME, https://www.bqprime.com/opinion/avnish-bajaj-redux-supreme-court-denies-relief-to-google-in-criminal-defamation-proceedings(last visited Mar. 8, 2023).

society at large from the potential dangers and difficulties presented by the digital environment. In general, Cyberlaw is essential to establishing a fair, secure, and safe online environment for all users.