IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyberlaws Everyone Using The Internet Should Be Aware Of.

[1]ANSHIT DUA, [2]VINAYAKA SRIVASTAVA

[1]STUDENT, [2]ASSISTANT PROFESSOR

[1]AMITY UNIVERSITY,

[2]AMITY UNIVERSITY

ABSTRACT

The internet has become an integral part of modern life, revolutionizing how individuals communicate, transact, learn, and conduct business. However, this digital transformation has also led to the emergence of serious cyber threats, including hacking, identity theft, phishing scams, cyberbullying, data breaches, and the spread of misinformation. In response to these growing challenges, countries worldwide, including India, have developed comprehensive legal frameworks known as cyberlaws to regulate digital conduct and ensure user safety. This paper explores the critical role of cyberlaws and emphasizes the urgent need for public awareness in the current digital landscape.

India's primary legal framework for governing cyberspace is the Information Technology Act, 2000 (IT Act), which defines cyber offenses and prescribes penalties. The paper outlines essential sections under the IT Act that deal with hacking (Sections 43 and 66), identity theft (Sections 66C and 72), phishing and online fraud (Section 66D), cyberstalking and harassment (Sections 66E and 354D), and cyberterrorism (Section 66F). These laws not only criminalize malicious activities but also empower individuals to protect themselves and seek legal remedies. Additionally, provisions like Section 65B of the Indian Evidence Act allow electronic records such as emails and messages to be used as admissible evidence in court, highlighting the growing importance of digital documentation in legal proceedings.

The paper further examines the evolution of data protection norms with the introduction of the Digital Personal Data Protection Act, 2023, and the relevance of Sections 43A and 72A of the IT Act, which mandate responsible handling of sensitive personal data. It also discusses the Personal Data Protection Bill, 2019, aiming to establish a Data Protection Authority and extend greater control to users over their digital information.

In addition to cybercrimes, the paper explores the significance of Intellectual Property (IP) laws, which protect digital creations such as music, art, software, and designs. Raising awareness about IP rights helps prevent unintentional infringements, fosters innovation, and ensures recognition for creators.

The study also focuses on the widespread issue of online financial fraud, including phishing, UPI scams, and fake investment schemes. By highlighting legal recourses and promoting digital literacy, individuals—especially vulnerable groups—can be better equipped to protect their finances.

Lastly, the paper addresses social media misuse, a growing concern in the digital age. Cyberbullying, identity theft, misinformation, and online defamation are prevalent on these platforms, necessitating user education and ethical digital behaviour.

INTRODUCTION

In today's interconnected world, the internet has transformed the way we live, work, learn, and communicate. From social networking and online shopping to banking, healthcare, and entertainment, the internet provides an extraordinary range of services at our fingertips. However, while the digital revolution has opened up countless opportunities, it has also given rise to a host of risks and vulnerabilities. Cybercrimes such as hacking, identity theft, online frauds, cyberbullying, data breaches, and the spread of malicious content have become alarmingly common. In response to these growing threats, governments around the world, including India, have introduced comprehensive cyberlaws to regulate and safeguard online activities.

Cyberlaws — also known as internet laws or digital laws — are the legal frameworks designed to protect individuals and organizations in the digital environment. They define legal standards for online behavior, ensure the protection of personal data, address criminal activities in cyberspace, and facilitate secure electronic transactions. In India, the cornerstone of cyber legislation is the Information Technology Act, 2000 (commonly referred to as the IT Act), which provides the basic structure for governing cyberspace activities. This Act, along with supplementary laws like the Indian Penal Code (IPC) and recent developments such as the Digital Personal Data Protection Act, 2023, forms the backbone of India's cyber legal ecosystem.[1]

The need for cyberlaws has become increasingly critical due to the rapid pace at which technology evolves. The internet is a borderless medium, where actions can have global impacts. A single act of cybercrime committed from one part of the world can have serious consequences for individuals, businesses, or even governments thousands of miles away. Therefore, a strong and dynamic legal framework is necessary not only to punish cybercriminals but also to create a secure digital environment that promotes trust, accountability, and ethical conduct online.

For everyday internet users, awareness of cyberlaws is essential. Many people unknowingly engage in activities online that could have legal implications. For example, forwarding a defamatory or false message on social media, downloading pirated content, or clicking on suspicious links can lead to serious consequences under cyberlaw provisions. Additionally, understanding one's rights — such as the right to data privacy, the right to protection against online harassment, and the right to seek redressal in case of cyber fraud — empowers individuals to act responsibly and seek timely help when faced with cyber threats.

Another important aspect of cyberlaws is their role in protecting businesses and the economy. With the rise of e-commerce, digital payments, and online financial services, securing electronic transactions has become a top priority. Cyberlaws provide the legal validity to electronic contracts, digital signatures, and online records, making business operations in the digital space reliable and enforceable. At the same time, they impose obligations on companies to protect customer data and maintain cybersecurity standards.

Social media has also added new dimensions to cyber law challenges. Online platforms have become breeding grounds for misinformation, hate speech, cyber stalking, identity theft, and online abuse. The legal provisions aim to strike a balance between protecting freedom of expression and preventing the misuse of online platforms. Users must understand that while expressing opinions is a right, spreading fake news, threatening others, or sharing obscene material is illegal and punishable under various sections of the IT Act and IPC.

Furthermore, the nature of evidence in legal proceedings has evolved with digitalization. Emails, WhatsApp messages, online transaction records, and even metadata are now considered electronic evidence and are admissible in court under Section 65B of the Indian Evidence Act. Hence, preserving digital trails and understanding how digital evidence can be used in legal disputes has become a critical part of cyberlaw knowledge.

[1] https://infosecawareness.in/cyber-laws-of-india

This research paper critically examines why cyberlaws play an indispensable role in shaping a safer, more trustworthy digital world. As more aspects of life move online, being ignorant of cyberlaws is no longer an option. Every internet user must be aware of basic cyber regulations to protect themselves, avoid inadvertent legal violations, and contribute to a secure and responsible digital society. Knowing your legal rights and obligations online is as important today as knowing your civil rights in the physical world. In the sections ahead, we will delve into the specific cyberlaws that every internet user should know, focusing on their significance, applicability, and the protection they offer in our increasingly digital lives.

WHY DO PEOPLE NEED TO KNOW ABOUT THE CYBERLAWS?

In the age of digital transformation, the internet has become a core part of everyday life. People use the internet for communication, business, education, entertainment, and even social activism. However, this increased dependence on digital platforms also brings with it a rise in cyber threats such as hacking, identity theft, online fraud, data breaches, and cyberbullying. In such an environment, awareness about cyberlaws has become not only important but essential. Cyberlaws provide a legal framework that governs the online world, and understanding them helps individuals protect themselves and others in the digital space.

Firstly, knowing cyberlaws enables people to safeguard their personal information. With the massive amount of personal data shared online—from social media profiles to banking credentials—cybercriminals constantly look for ways to exploit security gaps. Cyberlaws such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 in India define how data should be collected, stored, and protected.[2] Being aware of these laws helps users understand their right to privacy, what companies are legally allowed to do with their data, and how to report a data breach if it occurs.

Secondly, awareness of cyberlaws helps in preventing online crimes. Many users unknowingly engage in illegal online behavior simply due to a lack of knowledge. For example, downloading pirated movies, sharing fake news, or making offensive posts on social media can have serious legal consequences. By knowing what is permitted and what is prohibited online—such as cyberstalking, cyber defamation, and phishing—individuals can avoid committing punishable offenses and maintain respectful behavior online.

Thirdly, understanding cyberlaws empowers people to seek justice and legal remedies when they become victims of cybercrime. Whether it's a case of online financial fraud, identity theft, or cyber harassment, knowing the correct legal channels—such as reporting to cybercrime.gov.in or calling the cyber helpline 1930—can help individuals take timely action. Cyberlaws ensure that victims have the right to file complaints and that offenders can be punished under legal provisions.

Moreover, knowledge of cyberlaws is crucial for maintaining digital responsibility and ethical use of technology. As social media becomes a powerful tool for public discourse, users must understand the boundaries of free expression. Posting fake news, hate speech, or personal attacks can trigger legal action under IT and IPC sections. Hence, being aware of the consequences of online actions encourages more thoughtful and responsible internet usage.

In addition, cyberlaw awareness is vital in the professional and business world. Companies must comply with data protection norms, secure financial transactions, and ensure cybersecurity for customer trust. Employees also need to follow ethical and legal practices while using official networks and handling sensitive information.

In conclusion, in a world where every click can have serious implications, knowledge of cyberlaws equips individuals with the power to protect themselves, act responsibly, and contribute to a safe and lawful

[2] https://www.upguard.com/blog/cybersecurity-regulations-india

digital environment. Cyberlaw awareness is not just for IT professionals or law enforcement; it is a necessity for every internet user today.

INFORMATION TECHNOLOGY ACT, 2000 (IT ACT)

A. Data theft and hacking (sections 66 and 43)

Describe several kinds of hacking: unauthorized access, manipulation, and data theft. Talk about several methods hacking could happen (malware, vulnerability exploitation).

B. Hacking:

Section 43: Civil fines and pay-back for illegal access and hacking.

Section 66: Penalties for hacking under criminal law combining fines and incarceration.

Penalties:

Section 66 entitles one up to three years of imprisonment for hacking.

Fines under Section 66 run up to ₹ 2,00,000 fine.

Complicating international cybercrimes and demonstrating illegal access, prosecution of hacking cases presents challenges.[3]

C. Identity Theft (Sections 66c and 72)

Explore the idea of identity theft, in which a person utilizes another individual's personal information—such as passwords or PAN which are unlawfully for dishonest intent.

Legal system:

Section 66C: Deals with identity theft via illegal access to personal identification records.

Section 72: Deals with individual breaches by someone in a position of trust abusing private data.

Fines:

Section 66C: Fine ₹1,00,000 and imprisonment up to three years.

Section 72: Fine maximum ₹1,00,000; imprisonment up to two years.

D. Cybercrime and Phishing (Part 66d)

Talk about the several kinds of online fraud—phishing, vishing (voice phishing), and email scams. How cybercriminals pilfers sensitive data or money by means of deceit?

Legal provision:

Section 66D penalises cybercrime by impersonation and the use of false techniques to fool someone into revealing personal information or completing financial transactions.

Penalties consist:

[3] https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india

Up to three years of imprisonment plus fines up to ₹1,00,000.

E. Cyberstalking and Online Harassment (Sections 66e, 354d)

Cyberstalking and Harassment: Describe the phenomena of online harassment especially the use of social media platforms, emails, or messaging applications to stalk and harass someone.

Legal Frame:

Section 66E: addresses privacy violations resulting from the gathering and distribution of private pictures or videos.

Section 354D addresses cyberstalking within the framework of ongoing harassment by electronic means.

Penalties:

Section 66E: fines up to ₹2,00,000 and up to three-year imprisonment.

Section 354D: First offense carries up to three years of imprisonment; successive offenses carry five years.

F. Cyberterrorism Included In Section 66f

Describe the concept and extent of cyberterrorism—that is, the use of digital tools to target vital infrastructure, instill panic, or inflict general destruction.

Legal system:

Section 66F: Penalties for cyberterrorism; those found guilty of causing terror or major damage via cyber means face life in prison.

Punishments:

Life in jail as well as, in dire circumstances, the death sentence.

PERSONAL DATA PROTECTION AND PRIVACY

A. Sensitive Data Protection (Section 43A, Section 72A)

Given rising digital data sharing, highlight the need of safeguarding private information and the growing demand for legislation controlling this.

Legal clauses:

Section 72A addresses the invasion of privacy, especially with relation to the illegal publication of personal information by persons assigned to handle it.

Section 43A: Creates responsibility for businesses or entities failing to follow sensible security policies meant to safeguard data, especially personal information.

Penalty:

Section 72A: Fine up to ₹ 5 lakhs or imprisonment up to 3 years.

Section 43A: Data loss monetary reimbursement.

B. The 2019 Personal Data Protection Bill (PDPB)

Discuss the proposed Personal Data Protection Bill, 2019, which seeks to improve data privacy rights outside of what the IT Act provides.

Important clauses in the Bill consist in:

Establishing a Data Protection Authority. Improved rights for people over their personal information.[4]

Relation with the Information Technology Act: How the PDPB will enhance and expand the data protection mechanisms inside the Act?

LEGAL QUESTIONS AND ENFORCEMENT PROBLEMS

A. Jurisdictional Issues Regarding Cybercrime Cases

Cross-border Nature of Cybercrimes: Talk on how often cybercrimes cut over national borders and how international collaboration is required to properly fight these crimes.

Explain the challenges in enforcing cybercrime laws resulting from jurisdictional problems, lack of international treaties, and conflicting cybercrime laws across different countries.

Case Examples: Cases were perpetrators were outside India, so complicated the application of fines.

B. Technological and forensic difficulties in investigations on cybercrime

Lack of Cyber Forensic Experts: Talk about the difficulties investigating cybercrimes and the shortfall of qualified cyber forensic experts in law enforcement departments.

Technological Gaps: Talk about how quickly cybercrime strategies are changing and how law enforcement has to be always adjusting to new platforms, tools, and technology.

C. Insufficient Knowledge and Cyber security Norms

Public and Corporate Awareness: Emphasize how ignorance of cyber security among people and companies fuels the rising frequency of cybercrimes—especially data theft.

Training and Education: Talk about the need of raising knowledge of cyber security best practices among companies, in schools, and at the grassroots level.

INTELLECTUAL PROPERTY (IP) LAWS

Intellectual Property (IP) laws protect the creations of the human mind — inventions, literary and artistic works, designs, symbols, names, and images used in commerce. In the digital age, where content and creativity are shared rapidly across platforms, it is crucial for people to be aware of IP laws. Understanding these laws not only protects creators but also guides users on respecting the rights of others.

Firstly, awareness of IP laws helps people respect ownership rights. Many internet users often download music, movies, software, or images without realizing that unauthorized use of such material constitutes copyright infringement. By learning about IP laws, individuals understand that creators deserve recognition and compensation for their work, discouraging piracy and promoting ethical content consumption.[5]

[4] https://www.axiomlaw.com/guides/cyber-law

[5] https://www.cyberpeace.org/resources/blogs/growing-cyber-threats-in-india-policy-technology-and-public-awareness-

Secondly, IP laws encourage innovation and creativity. When people are aware that their original work — whether it's an app, a blog, a photograph, or a business logo — is legally protected, they feel more secure in sharing and monetizing their ideas. This legal protection fuels creativity and entrepreneurship, leading to a more dynamic economy.

Moreover, awareness of IP laws protects individuals from unintentional legal violations. For example, using a copyrighted logo without permission, replicating patented designs, or plagiarizing written content can attract legal consequences. People informed about IP rights can avoid costly lawsuits, reputational damage, and financial penalties.

For businesses and startups, understanding IP laws is critical. It helps them safeguard their brand identity, register trademarks, protect innovative products with patents, and create strong market positions. It also helps them respect the IP of others, thus avoiding legal disputes.

In the digital environment, where copying and sharing are easy, spreading public awareness about IP laws is vital for building a culture of respect, responsibility, and recognition. Schools, colleges, companies, and governments must promote education on IP rights so that every user becomes a responsible participant in the digital economy.

ONLINE FINANCIAL FRAUD

The rise of digital banking, online shopping, and mobile wallets has made financial transactions faster and more convenient. However, it has also opened the door to various forms of online financial fraud. These frauds include phishing scams, fake UPI links, credit card theft, online investment scams, and identity theft. As digital transactions become a part of daily life, public awareness about online financial fraud has become crucial for ensuring safety and protecting hard-earned money.

Firstly, awareness helps people identify and avoid common fraud tactics. Cybercriminals often use deceptive methods such as fake emails, calls, or text messages pretending to be from banks or payment platforms to steal sensitive information like OTPs, passwords, or bank details. Knowing how these scams operate enables users to recognize warning signs and avoid falling victim to them.[6]

Secondly, financial fraud awareness promotes safe digital habits. People learn the importance of setting strong passwords, enabling two-factor authentication, regularly monitoring bank statements, and using secure networks for transactions. These preventive measures significantly reduce the risk of financial loss.

Moreover, knowledge of legal protections and remedies is important. Laws under the Information Technology Act, 2000 and various provisions of the Indian Penal Code (IPC) provide ways for victims to seek justice. Platforms like cybercrime.gov.in and the 1930 Cyber Helpline allow individuals to report fraud quickly. Public awareness ensures that people know where and how to report suspicious activities and take immediate action if targeted.

Businesses, too, must be aware of financial fraud risks to protect their operations and customers. Secure payment gateways, compliance with data protection standards, and regular cybersecurity audits are essential for maintaining trust and legal compliance.

Additionally, financial literacy programs and government campaigns can play a big role in educating vulnerable groups — such as senior citizens and rural users — who may be less familiar with online threats. Community awareness drives can make digital financial spaces safer for everyone.

solutions

[6] https://legalonus.com/cyber-law-in-india-the-sentinel-of-the-digital-frontier/

SOCIAL MEDIA MISUSE

Social media platforms like Facebook, Instagram, Twitter, and WhatsApp have transformed the way people communicate, share ideas, and stay connected. However, these platforms are also increasingly misused for harmful activities such as cyberbullying, online harassment, spreading fake news, identity theft, defamation, and even inciting violence. In such a landscape, awareness about social media misuse is critical to ensure responsible usage and protect individuals from legal and emotional harm.

Firstly, awareness helps users recognize and avoid harmful behaviours. Many individuals unknowingly engage in illegal activities online, such as forwarding false news, sharing private images without consent, or making defamatory comments. Laws under the Information Technology Act, 2000 and Indian Penal Code (IPC) penalize such offenses. Educating users about the consequences of these actions can discourage misuse and promote a respectful digital environment.

Secondly, awareness empowers people to protect themselves from becoming victims. Cyberstalking, online blackmail, and identity theft are common on social media. Understanding how to use privacy settings, report abuse, and block offenders gives users greater control over their online safety. It also encourages early action if they face harassment or threats.

Moreover, awareness fosters critical thinking and digital responsibility. Fake news, hate speech, and misinformation spread rapidly on social media, often causing public unrest or damage to reputations. By promoting fact-checking habits and teaching people not to blindly forward unverified content, awareness campaigns can help curb the spread of falsehoods.

For teenagers and young adults, who are among the most active users, education about the risks of oversharing, online grooming, and peer pressure is vital. Schools, colleges, and parents have an important role to play in integrating social media literacy into education.

Businesses and influencers must also be mindful of legal and ethical standards while posting promotional content or engaging with audiences. Misleading advertisements or online defamation can lead to serious legal action.[7]

CONCLUSION

The rise of the internet and digital technologies has reshaped human life across all dimensions — communication, commerce, governance, education, and entertainment. While these innovations have brought unprecedented convenience, they have also exposed users to significant vulnerabilities, including cybercrimes, data breaches, financial frauds, and misuse of intellectual property. In such a rapidly evolving digital ecosystem, awareness and understanding of cyberlaws have become critical for every internet user.

This research has highlighted the crucial role of cyberlaws in safeguarding individuals and institutions in cyberspace. It discussed the significance of the Information Technology Act, 2000, and its key provisions related to hacking, identity theft, phishing, cyberstalking, and cyberterrorism. The importance of protecting personal data under laws such as Section 43A and the Digital Personal Data Protection Act, 2023, was emphasized, alongside the emerging framework of the Personal Data Protection Bill, 2019. Furthermore, the discussion extended to Intellectual Property (IP) laws, which protect creativity and innovation in the digital realm, and the critical need for public education on these rights to prevent misuse and encourage ethical behavior.

The increasing cases of online financial fraud and social media misuse further reinforce the urgency for widespread cyberlaw awareness. By understanding legal protections, safe online practices, and the

[7] https://vaquill.com/blog/cyber-law/

consequences of illegal activities, individuals can better protect themselves, act responsibly, and contribute to a safer digital environment.

So at last cyberlaw awareness is no longer optional — it is a necessity for survival and success in the digital age. Governments, educational institutions, businesses, and society at large must work collectively to promote cyber literacy, strengthen cyber security measures, and empower users with knowledge of their digital rights and responsibilities. Only through informed and responsible participation can we hope to build a secure, ethical, and resilient cyberspace for future generations.