INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 4 AND ISSUE 1 OF 2024

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Free and Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 4 and Issue 1 of 2024 (Access Full Issue on - https://ijlr.iledu.in/volume-4-and-issue-1-of-2024/)

Publisher

Prasanna S,

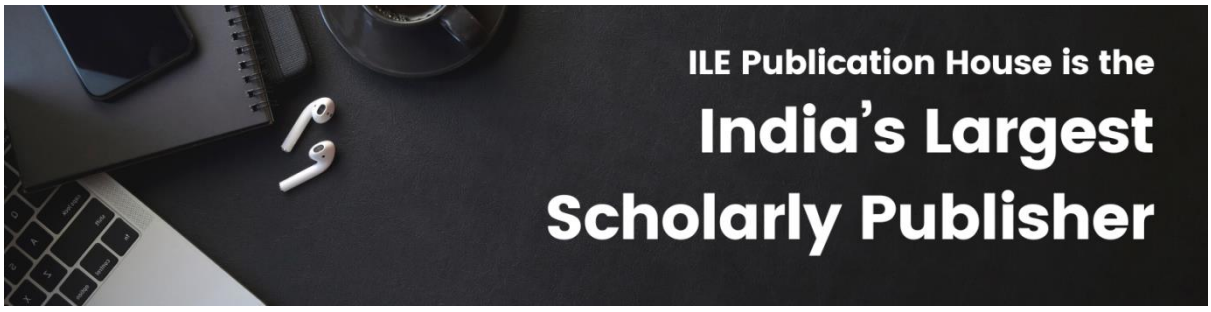
Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in



INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 1 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CYBER CRIME IN INDIA, ITS GENERAL OVERVIEW AND ALARMING RISE OF CYBERCRIME IN INDIA

AUTHOR - EVAN ALEX, STUDENT AT CHRIST UNIVERSITY

BEST CITATION – EVAN ALEX, CYBER CRIME IN INDIA, ITS GENERAL OVERVIEW AND ALARMING RISE OF CYBERCRIME IN INDIA, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 4 (1) OF 2024, PG. 579-590, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract:

In the global community of the future, the Internet is evolving into the town square. The Internet has now connected us all, much like neurons in a massive brain. Indeed, the internet has become both a blessing and a curse for modern society. These days, furthermore, as the requirement for the internet grows, safeguarding our data and information has also become essential. Regardless of whether you own a company, are a regular internet user, or something else entirely, you should know how to reduce risks, dangers, and cybercrime in addition to being proactive, careful, and aware of cybercriminals. Because of the development of technology, man now relies entirely on the internet. Man may now easily access everything while seated in one location thanks to the internet. The internet can be used for social networking, online shopping, data storage, gaming, online education, online employment, and anything else that comes to mind. Almost every field makes use of the internet. The idea of cybercrimes evolved along with the internet and all of its associated advantages. Cybercrimes take various shapes when they are committed. A few years ago, people were unaware of the atrocities that could be perpetrated online. When it comes to cybercrimes, India is catching up quickly to other nations where the frequency of these crimes is likewise rising daily. India saw a sharp rise in cybercrime cases in 2019 of 63.5%, according to the most recent government data. In India, the number of cybercrime cases increased dramatically by 63.5% in 2019. According to data from the National Crime Record Bureau (NCRB), there were 44,546 cybercrimes reported in 2019 compared to 28,248 in 2018. Karnataka (12,020) was the state with the most cybercrime cases, closely followed by Uttar Pradesh (11,416), Maharashtra (4,967), Telangana (2,691), and Assam (2,231). 78% of cybercrimes in the Union Territories were reported from Delhi.

Introduction

The use of a computer or computer network for illegal purposes is known as cybercrime. Any illegal behaviour involving a computer, computer network, digital device, or digital data might be classified as it.

Two main categories can be used to classify cybercrimes:

Crimes against property: These offenses are carried out with the goal of obtaining a person's assets, including cash, information, or creative works. These offenses include, for instance:

Identity theft is the theft of a person's credit card number, name, Social Security number, or other personally identifiable information.

Online fraud : The practice of using deceit to trick someone into giving you money or products. Phishing scams, pyramid schemes, and investment scams are a few instances of internet fraud.

Data breaches: These occur when private information, like financial, medical, or consumer details, is stolen or accessed without authorization.

Crimes against persons: These offenses are carried out with the goal of causing bodily or

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 1 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

emotional suffering to a victim. These offenses include, for instance:

Cyberbullying: Bullying someone online by sending scary or threatening messages is known as cyberbullying.

Online harassment: Persistently reaching out to someone without permission, usually with the goal of upsetting them.

Online child sexual abuse: The use of the internet to sexually abuse or exploit children is known as online child sexual abuse.

In India, cybercrimes are becoming a bigger issue. The National Crime Records Bureau (NCRB) stated in 2022 that the nation had over 5 lakh cybercrime cases on file.

The following were the most frequent categories of cybercrimes in India:

Online fraud: 1.9 lakh cases

Phishing: 1.5 lakh cases

Cyberbullying: 91,000 cases

Online harassment: 61,000 cases

Data breaches: 43,000 cases

Several measures have been implemented by the Indian government to tackle the problem of cybercrime these include:

- Enacting the Information Technology Act, 2000, which gives India's legal system a framework for handling cybercrime.
- The creation of the National Cyber Crime Reporting Portal, which enables Indian nationals to file online reports of cybercrimes.
- Establishing the Indian Cyber Crime Coordination Centre (I4C): This is a central organisation that aims to coordinate India's cybercrime investigation and prosecution processes.

But even with these precautions, cybercrime is still a significant issue in India. The nation is a prime target for hackers because to its sizable and expanding internet population, lack of awareness about cybercrime, and other factors.

Objectives of the study

The specific objectives of the evaluation study include the assessments / examination of the

following:

1. The meaning of cybercrime and its kinds

3. The portray as to what extent the cybercrime is increasing in India

3. To identify the role of government in order to fight with the cyber crime

4. To identify the major cases of cybercrime in India.

5. To portray how to prevent cybercrime in India.

6. To identify Cyber Security Measures for Organizations to Prevent Cyber Attacks

Research Questions:

1. What is the meaning of cybercrime?

2. What are different types of cybercrime?

3. What are major cybercrimes happened in India?

4. What are the security measures for organizations to prevent cybercrime?

5. Cybercrime in other countries and its punishments?

Cyber Laws

Information Technology Act (IT Act) (2000)

The United Nations Commission on International Trade Law's Electronic Commerce Model Law served as the model for the Information Technology Act (IT Act), which India passed in 2000. The IT Act recognizes electronic trade and permits businesses and government organizations to submit electronic documents to the government. The Act protects both Indian citizens and foreign nationals whose crimes are covered by the Act. It is applicable across the country. The IT 2000 Act also includes cybercrimes performed outside of India, provided that the offense involves computers,

computer systems, or networks operated within India, due to the cross-border character of these crimes. In addition to security procedures, offenses, the role of investigative authority, penalties, and adjudications, it provides definitions for terms like computer network, digital signature, private key (a pair of keys used to create digital signatures), public key (a pair of keys used to verify digital signatures), breach of confidentiality and privacy, and more (Ministry of Law, Justice and Company Affairs 2000).

The 2000 IT Act includes several offenses, such as tampering with computer documents, loss or damage to computer resources, hacking, publishing of pornographic materials electronically, companies' refusal to help decrypt the information intercepted by the government, unauthorized access to computer systems, obtaining licenses or Digital Signature Certification (DSC) through deception, publishing false or fraudulent DSC, and breach of confidentiality (Dubbudu 2016).

Investigatory authority is granted to police officials who hold the position of deputy superintendent of police or above.

According to the Act, if an officer has a reasonable suspicion that an individual has committed an infraction, they may search a public area without obtaining a warrant. Data Security. Chapter IX (Penalties and Adjudication) of the IT 2000 Act, Section 43, lays out the following civil (i.e., monetary) penalties: (1) unauthorised access to any computer, computer system, or network; (2) downloading, copying, or extracting any data or information; (3) introducing a virus into any computer, system, or network; (4) causing damage to any computer, system, or network; (5) disrupting any computer, system, or network; (6) denying access to any computer, computer system, or network; (7) offering assistance to someone who is not authorized to access a computer system; and (8) tampering or manipulating any computer or network, or computer system. Violators are subject to damages of up to Rs. 1 crore, or $140,000 USD. The Cyber Regulations Appellate Tribunal was established under the Act to decide cases involving violations of the Act. The Tribunal will consist of a High Court judge or an Indian Legal Service member with a specific level of expertise and rank. The Ministry of Law, Justice, and Company Affairs (2000) states that the Tribunal's processes and authority are comparable to those of a civil court. Additionally, the Act made it easier to change the Reserve Bank of India Act (1934), the Indian Evidence Act (1872), the Indian Penal Code (1860), and the Bankers' Books Evidence Act (1891) (Ministry of Law, Justice, and Company Affairs 2000).

Information Technology (Amendment) Act (ITAA) (2008)

The 2000 IT act only had 10 chapters, which Nappinai (2010) states "fell short of the industry's requirements to meet global standards." Furthermore, the absence of criminal provisions in the IT Act made it impossible to prosecute crimes including virus attacks, illegal access to or removal of data, and data theft. The lack of focus on cybercrimes against women and children, like pedophilia and cyberstalking, has also drawn criticism. The IT Amendment Act (ITAA) of 2008 was passed in spite of opposition to the suggested draft modifications of 2005 and 2006. According to Nappinai (2010), the ITAA was enacted in a "knee-jerk" response to the terrorist attack that occurred in Mumbai in November of 2008.

Despite objections, the ITAA (2008) significantly expanded the field of cyberlaw. According to Ministry of Law and Justice (2009), p. 2, "computer network" is defined as "inter-connection of one or more computers or computer systems or communication device through..." using wire, wireless, satellite, or microwave as well as any other communication means. It expanded the scope of communication devices by substituting the word "electronic" for "digital," which covered cell phones and other electronic devices. All service providers were included in the definition of

"intermediary," expanding its meaning. According to the Ministry of Law and Justice (2009), the Act further broadened the definition of "cybersecurity" to encompass any "unauthorized access, use, disclosure, disruption, modification, or destruction" of any computer, computer resource, equipment, or communication device.

The New Features of the Act

Information Security: Under ITAA (2008). Procedures for data protection were added in response to industry demands. Section 43A mandates that "body corporates," which include businesses, sole proprietorships, and associations engaged in commercial or professional operations, maintain appropriate security measures to thwart illicit activity, damage, and unauthorized access. They may face both civil and criminal penalties if they neglect to maintain "reasonable security practice and measures" (Ministry of Law and Justice 2009).

Privacy and Confidentiality: Regarding privacy, see Section 66E. A person's privacy is breached if they purposefully or knowingly take a picture of, publish, or transmit without authorization of any private region of that person (such as their buttocks, female breasts, or partially or completely exposed genitalia) in electronic form. Therefore, revenge pornography is forbidden by Section 66E's privacy and confidentiality rules. Such a violation carries a maximum sentence of three years in prison, a maximum fine of two lakhs rupees, or both. An intermediary or anyone performing services under a contract who divulges personal information with the aim to injure or unlawfully benefit is covered by Section 72A, which extends the coverage and carries a maximum sentence of three years in prison.

Child pornography and materials with explicit sexual content: While most ITAA infractions carry a two-to three-year prison sentence, Section 67A of the law punishes the electronic publication or transmission of sexually explicit content with a five-year prison sentence and a fine. Similarly, it is illegal to record one's own abuse in any electronic format, facilitate online child sexual abuse, entice or induce children to have an online relationship with other children for transmitting images of sexually explicit acts, or depict children in a sexually explicit manner. These actions can result in up to five years in prison and a fine of up to Rs. 10 lakhs. A fine of up to Rs. 10 lakhs and a maximum sentence of 10 years in prison could be imposed for any further conviction. Also, any intermediary who violates the provisions of the Act is liable and may receive the punishment of up to 3 years in prison and a fine.

Cyber terrorism: Section 67F defines cyber terrorism as any act that aims to "threaten the unity, integrity, security or sovereignty" of the nation or instil fear in the populace. This includes the following: (1) preventing authorized users from accessing computer resources; (2) allowing unauthorized users to access resources after their authorization has expired; (3) introducing viruses or other contaminants; (4) using methods that may or may not result in property damage, disruption of essential community supplies or services, or death or injury to individuals; or (5) negatively affecting the critical infrastructure (Ministry of Electronics and Information Technology 2009). Cyber terrorism offenses, including conspiracy to commit, carry a life sentence in jail. Furthermore, the ITAA gave the investigative powers to officers in the rank of an inspector or above, expanding the enforcement powers in investigating cybercrimes.

Government Authority and Data Interception: The appropriate agency may be directed by the federal government, a state government, or any officer designated by the government "to intercept, monitor, or decrypt... any information generated, transmitted, received, or stored in any computer source" in accordance with Section 69 of the ITAA (Ministry of Electronics and Information Technology 2009, p. 12). If a subscriber or middleman declines to cooperate with such authority, they risk a fine and/or up to seven years in prison. Furthermore, it grants the

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 1 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

government the authority to order the blocking of any computerized public information if it deems it necessary to safeguard national security and defence, maintain good relations with friendly countries, or preserve the nation's sovereignty or integrity.

Cybercrime Statistics

Cybercrimes in India are included in the NCRB's annual Crime in India report, as was previously mentioned. The IT Act, IPC, and SLL are the three main legal frameworks that cover cybercrimes. The NCRB began recording cybercrimes in 2002, and since then, the number of cases filed under the IT Act has increased dramatically. For instance, in 2002, 738 cases were registered under the IPC and 70 cases under the IT Act. By 2016, the number of IT cases had risen to 8,613. Similarly, by 2016, there were 3,518 IPC crimes (using a computer) 12,317 cybercrimes were reported overall in 2016 (NCRB 2016).

Cybercrimes recorded under IT Act, IPC, and SLL, 2016

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 1 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

ercriminals' motivations, and the state of the investigation. Among the stated motivations are extortion/blackmail, sexual exploitation, insulting women's modesty, retaliation, and illicit wealth. Other stated mot

The types of violations and cases under the IT Act, IPC, and SLL that were registered in 2016 are displayed in table . The NCRB also gathers data on court rulings, cyb

Offenses	Cases
IT Act offenses	
Tampering with computer source documents	78
Computer-related offenses (Sec 66, 66B–E)	6,818
Other IT cybercrimes	12
Publication/transmission of an obscene/sexually explicit act in the electronic form	957
Breach of confidentiality/privacy & disclosure of information	35
Other cybercrimes	713
Total	8,613
IPC offenses	
Data theft	86
Criminal breach of trust/fraud	56
Cheating	2,329
Forgery	81
Counterfeiting	10
Fabrication of false evidence/destruction of electronic records	6
Other IPC offenses	950
Total	3,518
SLL offenses	
Copyright Act	181
Trademark Act	2
Other SLL Offenses	3

ivations include causing embarrassment, growing a business, pulling pranks or feeling satisfied with taking control, political motivation, interfering with public services, piracy, stealing information for espionage, buying or selling illegal narcotics and other products, and inspiring hatred against the nation. There are further causes that NCRB has not yet recognized. Out of all the stated motivations, the top five were: extortion/blackmail, sexual exploitation, unlawful gain, retaliation, and insulting women's modesty. Some understanding of the motivations behind these crimes can be gained from the statewide breakdown of cybercrimes. The northern Indian state of Assam ranked highest for cybercrime motivated by political or retaliatory goals. The state of Uttar Pradesh, which is in north-central India, has the largest number of blackmail and "hate crimes against a community" events. The state "has an infestation of trolls as it also tops the list where the motive is 'Prank/Satisfaction of Gaining Control' Police data on cybercrimes indicates that 24,187 cases were looked at in total in 2016, with 11,870 of those cases still awaiting investigation from the year before. Police resolved 9,213 (40.3%) cases in total in 2016; 14,973 (61.9%) cases remained unresolved. These figures suggest that in order to finish the investigations on time, more investigating officers are required.

Disposal of cybercrimes by court, IT Act., IPC, and SLL

Offenses	Persons convicted	Persons acquitted	Persons discharged
IT Act			
1. Tampering with computer source documents	1	15	0
2. Computer-related offenses	172	370	14
3. Cyberterrorism	0	0	0
4. Publication/transmission of obscene/sexually explicit content	12	53	1
5. Breach of confidentiality/privacy & disclosure of information	0	1	0
6. Others	17	33	2
Subtotal	202	472	17
IPC			
1. Data theft	0	6	0
2. Criminal breach of trust/fraud	0	2	0
3. Cheating	6	37	1
4. Forgery	0	32	0
5. Counterfeiting	0	1	0
6. Fabrication/destruction of electronic records for evidence	0	0	0
7. Other	15	48	0
Subtotal	21	126	1
SLL			
1. Copyright Act, 1957	31	96	0
2. Trademark Act, 1999	0	0	0
3. Other SLL Offenses	0	1	0
Subtotal	31	97	0
Total	254	695	18

The number of people found guilty, cleared, or released is displayed in the table. 202 (29.2%) of the 691 people who were tried by the courts or tribunals under the IT Act were found guilty; the remaining cases ended in dismissals or acquittals. Out of

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 1 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

the 148 individuals who were tried for IPC violations, just 21 (14.2%) were found guilty. 128 persons were tried by the courts or tribunals for SLL offenses, and 31 of them (24.2%) were found guilty. 26.2% of the total were found guilty. Once more, the low conviction rate points to the necessity of judges with specialized training to deal with cybercrime.

Gender and Cybercrimes

Compared to men (n = 5,879; 98.6%), a lower proportion of women (n = 85; 1.4%) were arrested in 2016 under the IT Act. 33 women and 3,381 men were charged out of those who were taken into custody. Regarding IPC violations, 1,727 (96.8%) males and 58 (3.2%) women were placed under custody; 43 women and 1,228 men were charged. Compared to 237 (98.3%) men, only four (1.7%) women were arrested for SLL violations; charges were brought against all four women and 224 men. Women were represented in every category of charges under the IT Act, with the exception of cyber terrorism, where seven men were taken into custody. Similarly, women were detained for most IPC violation categories, with the exception of data theft and the creation or destruction of electronic documents.

Cybercrimes against Women.

Cybercrimes against women in India are not formally recorded. Due to the increase in crimes against women, including rape and domestic abuse, cybercriminals are also using online platforms as additional means of intimidating women. Cybercrimes include "trolling, threatening, stalking, voyeurism, body-shaming, defamation, surveillance, revenge porn and other forms of indecent representation" have affected women. (Page 1 of Kapadia (2018)). "Trolls" are defined as people who, using a computer resource or communication device, spread false or inflammatory messages about other people that are "grossly offensive or has menacing character… for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently .disseminate divisive messages in an online community via blogs, chat rooms, and forums to emotionally abuse the victim.

Also, the number of women complaining of being blackmailed by their ex-husband has been on the rise. Sexual offenses against women and children are also a result of online bullying, stalking, and grooming of these victims. It becomes challenging for law enforcement to find the people responsible for uploading pornographic or sexually explicit content to the internet. Furthermore, the content—whether written or visual—tends to resurface frequently on the Internet and is difficult to erase. In the 2012 case Karan Girotra v. States and Others, the petitioner submitted an application for anticipatory bail (a person accused with a felony that is not bail able may request bail in advance of an arrest under Section 438 of the Code of Criminal Procedure). Regarding a case brought under the ITAA's Sections 328 (using poison to cause harm) and 376 (punishment for rape), as well as Section 66A. In this instance, Ms. Shivani Saxena reported to the police that she was married to Ishan, but the marriage did not work out since her husband was unable to consummate the union. They chose to get a divorce. Subsequently, she connected with Mr. Karan Girotra online. He declared his desire to wed her after declaring his love for her. He invited her to his house, drugged her, and sexually assaulted her. She also alleged in her complaint that the petitioner threatened to distribute nude and obscene pictures of her if she did not maintain a physical relationship with him. He ended their engagement, even though they were engaged. The court observed that Ms. Saxena's complaint was not filed right away. Saxena had a consensual relationship with Girotra; the court dismissed the sexual assault and ruled that she only made a complaint after Girotra called off their engagement. This case exemplifies the Indian judiciary's attitude toward women.

Halder and Jaishankar (2017) state that little is known about data mining on adult dating services. But it appears that marriage-related

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 1 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

websites are replacing dating sites. These websites allow prospective brides and grooms to upload personal information, but they don't offer much privacy protection. Fraudsters approach ladies by posing as someone else. An "Advisory on the functioning of matrimonial websites in accordance with the Information Technology Act, 2000, Rules" was released in 2016 by the Ministry of Communications and Information Technology to address the problem of fraud and information misuse (Ministry of Communications and Information Technology 2016, p. 1). All matrimonial websites and mobile applications are covered by the recommendation. Due to their status as middlemen for any electronic records they hold, these marriage-matching websites are required to abide by the IT Act's regulations as well as other government directives (Ministry of Communications and Information Technology, 2016).

Cybercrimes against Children.

Crimes committed against minors are on the rise in India. Every second child has experienced some form of sexual abuse at some point in their lives, according to the Ministry of Women and Child Development (2007). There was a 500% increase in crimes against kids between 2006 and 2016, according to the nongovernmental organization Child Rights and You (CRY 2016). Following a comprehensive nationwide study by the Ministry of Women and Child Development in 2007 that detailed the types and scope of child abuse for both genders, the Indian government passed the Protection of Children from Sexual Offenses Act (POCSO Act of 2012), a comprehensive piece of legislation. The NCRB was required by this Act to record offenses against minors as a distinct category. Prior to the POCSO Act, the NCRB grouped crimes with other offenses, with the exception of child rape. According to Dey (2015), serious crimes against minors include infanticide, rape, kidnapping, and trafficking. The fact that thieves may now target youngsters over the Internet only serves to exacerbate the issue. According to Halber and Jaishankar (2017)[10], cybercriminals "groom their victims to contribute to the victimization." In addition, groomers either hurt other people or use their victims as pawns to lure in new victims. The explicit prohibition against the electronic publication or transmission of any sexually explicit act or activity involving children is stated in Section 67B of the ITAA (2008). If found guilty, anyone who writes or creates digital images, downloads, browses, advertises, promotes, or distributes sexually explicit content of children or entices children for sexual purposes online, helps facilitate child abuse online, or records their own or others' abuse and shares it online faces a maximum five years in prison and a fine. If convicted again, the penalty would be increased (Ministry of Law and Justice, 2009).

(Karan Girotra vs State & Anr.)[8]

(Information Technology Act, 2000)[9] Halder, Debarati and Jaishankar, K., Cyber Victimization in India: A Baseline Survey Report (2010) (December 1, 2010). [10]

Conclusion

Given India's growing reliance on information technology and digitalization, cybercrime has become a serious threat to the nation. Cybercriminals' strategies and techniques also evolve with technology. This article will look at India's current cybercrime situation, the difficulties it poses, and some ways to reduce the threats.

State of Cybercrime Right Now:

In recent years, cybercrime has steadily increased in India, affecting private citizens, commercial enterprises, and governmental institutions. Financial fraud, data breaches, identity theft, online harassment, and cyberbullying are examples of common cybercrimes. These cybercrimes have a variety of motivations, from political and ideological to pecuniary.

India faces significant hurdles in battling cybercrime due to the swift growth of the digital realm. More Indians have access to online

platforms due to the widespread use of cellphones and the internet, which makes them possible targets for cybercriminals. Furthermore, insufficient cyber security protocols, both personal and organizational, provide weaknesses that cybercriminals take advantage of.

Difficulties in preventing Cybercrime:

Lack of Knowledge: In India, a large number of people and institutions are ignorant of the dangers posed by cybercrime. This ignorance may result in a carelessness with the application of fundamental cyber security procedures, leaving them open to intrusions.

Underreporting: There are a number of reasons why cybercrimes are frequently not reported, such as uncertainty about the effectiveness of law enforcement, fear of social shame, and ignorance of the reporting procedure.

Inadequate Law: The Information Technology Act of 2000 has strengthened India's legal framework in the country's fight against cybercrime. Nonetheless, the Act still has some holes and ambiguities that need to be filled.

Cyber security Skills Deficit: In India, there is a dearth of qualified cyber security experts. This disparity makes it more difficult to properly protect against cyber-attacks.

Cross-Border Nature: Since many cybercrimes include foreign parties, it might be difficult to identify and apprehend those who operate from locations outside than India.

Possible Remedies:

Raising Awareness and Education: From corporations to schools, there should be campaigns to increase public knowledge of cyber security. This will support the adoption of best practices by people and organizations to safeguard themselves.

Strengthening Law: In order to combat changing cyber threats, the government should update and reinforce the law on a regular basis. This entails precise descriptions of cybercrimes, severe punishments, and protocols for documenting and bringing criminals to justice.

Enhanced Law Enforcement: It is essential to fund law enforcement agencies' capacity-building and training initiatives in order to effectively combat cybercrime. State and federal governments can create specialized cybercrime units.

Public-business Partnerships: To effectively address cybercrime, cooperation between the public and business sectors as well as civil society is necessary. Sharing threat intelligence and best practices is something that private organizations should actively engage in.

International Cooperation: India should collaborate with other nations and international organizations to exchange information and extradite offenders due to the cross-border nature of cybercrimes.

Research and Development in Cyber security: To keep ahead of new threats, promote cyber security research and development. Industry cooperation and government incentives can support the growth of this sector.

Digital literacy: Encouraging people to be digitally literate will enable them to identify possible risks, stay safe online, and report instances.

In conclusion, cybercrime is becoming a bigger issue in India and calls for a multifaceted response. Important steps in reducing cyber dangers include raising awareness, enacting laws, assisting law enforcement, and fostering international collaboration.

References

n.d. <https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfg>.

n.d. <https://rajasthanjudicialacademy.nic.in/docs/studyMaterial05022021.pdf>.

n.d. <https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf>.

Bibliography

Brush, K., & Cobb, M. (2024, January 2). *Cybercrime*. Security. https://www.techtarget.com/searchsecurity/definition/cybercrime

P. (2021, November 14). *Over 400% rise in cybercrime cases committed against children in 2020: NCRB data*. The Economic Times. https://economictimes.indiatimes.com/news/india/over-400-rise-in-cyber-crime-cases-committed-against-children-in-2020-ncrb-data/articleshow/87696995.cms?from=mdr

Kethineni, S. (2020). Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms. In: Holt, T., Bossler, A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_7