REVISTA
BRASILEIRA DE DIREITO

A timeline analysis of cybercrime and cyberattacks with reference to judicial pronouncements

Uma análise cronológica da cibercriminalidade e dos ciberataques com referência aos pronunciamentos judiciais

Arpit Sharma(1); Sharad Kumar Pandey(2); Ravi Dubey(3)

1 Assistant Professor, Institute of Law, Nirma University, Ahmedabad, India.
E-mail: arpitt.sharmaa@gmail.com | ORCID: https://orcid.org/0000-0001-8883-260X
2 Research Scholar, Department of Law, School of Legal Studies, Babasaheb Bhimrao Ambedkar University, Lucknow, India. E-mail: sharadpandey111@gmail.com | ORCID: https://orcid.org/0009-0001-3798-0757
3 Research Scholar, Department of Law, Dr. Ram Manohar Lohiya National Law University,Lucknow, India.
E-mail: ravi23dubey@gmail.com | ORCID: https://orcid.org/0009-0004-5520-1923

Revista Brasileira de Direito, Passo Fundo, vol. 19, n. 3, e4986, September-December, 2023 - ISSN 2238-0604
[Received: april 12, 2024; Accepted: june 11, 2024;
Published: june 27, 2024]
DOI: https://doi.org/10.18256/2238-0604.2023.v19i3.4986

Como citar este artigo / How to cite item: clique aqui!/click here!

Abstract

This article aims to comprehend cybercrime in cyberspace and how the government-authorized agency and judiciary are taking steps to prevent these types of cybercrime where the offenders hide beside the algorithms. This work aims to disseminate how the numbers are increasing in cyber-crimes and to take preventive measures against them. In this study, the data on cybercrimes and their variation are analyzed related to cyber-attacks from 2017 to 2021 and analyzed judicial decisions. The study on cyber-attacks helps the policy maker to framework it is regulation based on the outcome wherein the creation of using the digital platform can be one of the most acceptable contributions to preventing cyber-crimes. This work adds value to the authorized agencies wherein the judiciary interpretation helps them use framework guidelines/alerts to take preventative measures. The finding of this paper depicts that the increased usage of cyberspace leads to an increase in cybercrime, wherein the concept of creating sensitization to use the digital mode and create awareness is essential. The government agency should introduce training centers to create awareness, and more volunteers should be added to these agencies for preventive exercise.

Keywords: Cyber-Crime; Cyber-attacks; Legal provisions; Scams.

Resumo

Este artigo tem como objetivo compreender o cibercrime no ciberespaço e a forma como a agência governamental autorizada e o sistema judicial estão a tomar medidas para prevenir este tipo de cibercrime em que os criminosos se escondem ao lado dos algoritmos. Este trabalho visa divulgar como os números estão a aumentar nos crimes cibernéticos e tomar medidas preventivas contra eles. Neste estudo, são analisados os dados sobre os cibercrimes e sua variação relacionados aos ciberataques de 2017 a 2021 e analisadas as decisões judiciais. O estudo sobre ataques cibernéticos ajuda o formulador de políticas a enquadrar sua regulamentação com base no resultado em que a criação do uso da plataforma digital pode ser uma das contribuições mais aceitáveis para a prevenção de crimes cibernéticos. Este trabalho acrescenta valor às agências autorizadas, sendo que a interpretação judicial ajuda-as a utilizar directrizes/alertas de enquadramento para tomar medidas preventivas. A conclusão deste trabalho mostra que o aumento da utilização do ciberespaço conduz a um aumento da cibercriminalidade, pelo que é essencial o conceito de sensibilização para a utilização do modo digital e de consciencialização. A agência governamental deve introduzir centros de formação para criar consciencialização, e devem ser acrescentados mais voluntários a estas agências para o exercício preventivo.

Palavras-chave: Cibercrime; Ciberataques; Disposições legais; Fraudes.

1 Introduction

The term 'attack' has gained momentum in the cyber world, broadening the horizon of the term attack linked as a war; terrorism nowadays is linked with cyber-attacks. The traditional attacks, which can identify as war, can be regulated by the law of war. In contrast, cyber-attacks have widened up in the form of virtual attacks where the jurisdiction of tracking has no significance. This article examines how these cyber-attacks can be regulated and how the agencies create an algorithm and awareness among the users to create cyber security. In the present era where data and information play an essential role for government agencies, business organizations, financial institutions, and universities where the control simulations and data have confidential information to be secured from being attacked. The challenges behind the experts cannot be mitigated through domestic reform. It required international cooperation.

United Nations took up the international framework on cyber-attacks under the head of the 'Global Programme on Cybercrime'[1] for creating a capacity-building program among the nations and sharing best practices which include technical assistance. The challenges arise due to the uncodified definition of 'cyber-crime' where the offenses arise against confidentiality and integrity, ranging from copyright infringement and other laws. The cyber-world raises the alarm that many illegal activities are run by experts and recognized by many research centres, including the dark web and other cyber-attacks in the virtual world.

2 Review of Literature

In his research, the author[2] emphasizes the type of scams that have resulted in the target group of 20-29 years by doing technical tricks on social media and other platforms. The author provides the solution for preventing or reducing cyber-attacks by sensitizing the awareness program related to technology usage. The major challenge in tracking the cyber-attacker is recognizing the doer of these attacks. The author cited the data, showing that children, women, and senior citizens are more vulnerable to cyber-attacks.

The author[3] in this article emphasizes the growth of cyber-crimes in India and how the government has taken measures to curb these issues. The author cited the

1 UNITED NATIONS. *General Assembly resolution 65/230 and Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8*. Available in: Global Programme on Cybercrime (unodc.org). Accessed: may, 5, 2022.

2 DATTA, Priyanka *et al*. A technical review report on cyber crimes in India. *In*: *2020 International conference on emerging smart computing and informatics* (ESCI). IEEE, 2020. p. 269-275.

3 KUMAR, Vijaya. Growing cyber crimes in India: A survey. *In*: *2016 International Conference on Data Mining and Advanced Computing* (SAPIENCE). IEEE, 2016. p. 246-251.

literature with evidence that in 2013, India ranked top five leading countries for cyber-crime. The study focused that most of these cyber-crimes are related to financial services under the banking or digital payment structure wherein the government enacted several laws and authorities to report the matters and take appropriate actions.

The author[4] covers the significance of cyber security against cyber attacks and its impact on reducing cyber-crime. The study suggested the positive result of using cyber security tools in an organization and creating public awareness against these cyber crimes. The author concludes that digitalization in India increases the opportunity for cyber attackers to trap vulnerable groups and create scams against them. The only solution to this problem is to create awareness at the same pace as the identified scammer activities.

This article's author[5] emphasizes that cybercrime is becoming a significant threat. Governments, police forces, and intelligence agencies worldwide have begun to respond. Initiatives to reduce international cyber threats are beginning to take form. The Indian police have established specialized cyber cells nationwide and have begun training the staff. This essay aims to provide readers with a glimpse of cybercrime in modern culture. This article is based on numerous news articles and news portal stories.

In this work, the author[6] focuses on internet transmission of vast amounts of information is essential in this information and technological age. It affects all aspects of human life and all adult age groups. Even if the internet has radically altered our society, there is still a risk of unauthorized access to and damage to online information. Cyber security and safety are now the most significant concern facing society today. The number of cybercrime cases is rising quickly alongside the number of users, and national or geographic borders do not constrain them. India has experienced many cybercrime cases during the last few years. The author concludes the research that the number of cybercrime instances in various Indian states and towns has steadily increased over the past ten years. A relatively more minor number of people have been detained concerning reported cybercrime instances. Therefore, it is evident that there are still some problems with our cyber frameworks and Indian cyber laws, as our Information Technology Act cannot wholly protect our online environment.

The authors[7] of this work focuses on cyberattacks as a growing aspect of IoT and impacts user lives and society, so substantial measures must be taken to protect

4 KUMAR, Vijaya. Growing cyber crimes in India: A survey. *In*: *2016 International Conference on Data Mining and Advanced Computing* (SAPIENCE). IEEE, 2016. p. 246-251.

5 DASHORA, Kamini. Cyber-crime in the society: Problems and preventions. *Journal of Alternative Perspectives in the social sciences*, v. 3, n. 1, 2011. p. 240-259.

6 KARALI, Yalcin et al. Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India. *International Journal of Engineering and Management Research* (IJEMR), v. 5, n. 2, 2015. p. 43-48.

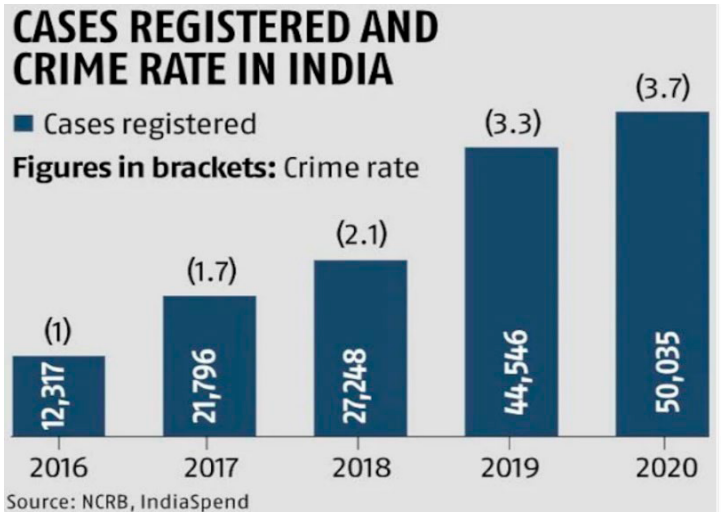
7 MUGWENI, Benison; MUGWENI, Rose. New Patterns in Cyber Crime with the Confluence of IoT and Machine Learning. *In*: *ICT and Data Sciences*. CRC Press, 2022. p. 117-133.

against them. Cybercrimes can harm consumers in a variety of ways and pose a threat to the infrastructure of governments and corporations around the world. Various measures are being tried to impede these attacks, but sadly they have not been very successful thus far. Therefore, safe IoT is necessary for this day and age, and it is crucial to study the dangers and assaults against IoT systems. Cyberattacks can occur for several reasons, including weak cyber security measures in some countries—secondly, cybercriminals using new attack technology. Thirdly, services and other business plans make cybercrime viable.

3 Increase of Cyber Crime in India

India has witnessed a sharp surge of cyber-crime cases, incidentally due to an increase in technological usage and dependency on transactions through the digital platform. During the pandemic, the rate of incidents increased sharply, and cyber cells received many complaints for crimes committed through technology. The data pattern shows that cyberspace is used for fraud ranging from money transaction fraud to the circulation of fake news on social media.

Figure 1. Cases Registered and Crime Rate in India



Source: Business Standard[8]

Fig 1. depicts that there has been a sharp rise in cybercrime e cases in the past five years, and it raises the concern of creating cyber awareness to the public at large to reduce the crimes in cyberspace. The surge in the numbers is directly linked to the usage of digital platforms, which shift the crime paradigm. The government is creating public announcement/security alerts for cyber security mechanisms so that

8 BUSINESS STANDARD. *India registered 136 cybercrime cases every day in 2020*: NCRB data. India, february, 21, 2022. Available in: https://www.business-standard.com/article/current-affairs/india-registered-136-cybercrime-cases-every-day-in-2020-ncrb-data-122022100007_1.html. Accessed june, 10, 2022.

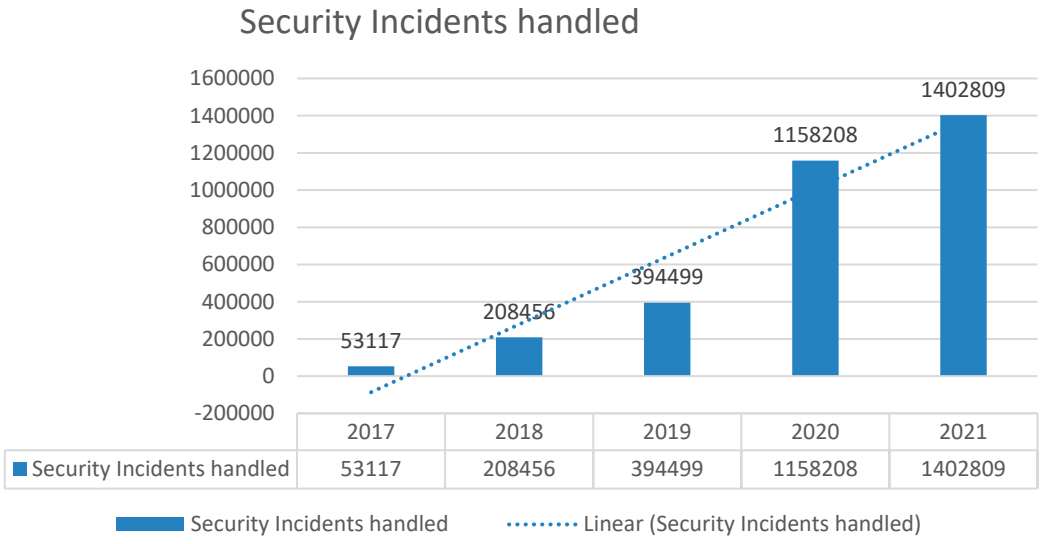
the digital user may not be trapped in cyber-crime. The data of reported cybercrime in the year 2020 is 50 035, which means around 138 reported incidents are there every day, whereas many surveys so that many incidents are unreported due to a lack of awareness on how and to whom they will be approached. The answer to this question is to create awareness through the training program, issuing public alerts, demonstrating videos on public portals, etc.

3.1 Mechanism of the Indian Computer Emergency Response Team (CERT-in) for Cyber Attacks

The Ministry of Electronics and Information Technology of the Government of India operates CERT-In to protect Indian cyberspace. CERT-In offers incident deterrence and retorts services along with security quality management services. According to the Information Technology Act of 2000, CERT-In is the official national agency for carrying out the following tasks in the field of cyber security are as follows:

- Collecting, analyzing, and sharing data on cyber incidents
- Cybersecurity incident forecasts and warnings alerts
- Immediate responses to cyber security incidents
- Coordination of cyber incident response operations, the publication of advisories, vulnerability notes, and whitepapers on information security policies, protocols, the prevention, response, and reporting of cyber incidents, as well as any other prescribed cybersecurity-related duties.

Figure 2. Security Incidents Handled reports (2017-2021)



CERT-In features Services that help organizations safeguard their systems and networks, including advisories, security alerts, vulnerability notes, sharing of indicators of compromise, situational awareness of current and potential cyber security threats, and security guidelines. Reactive services to reduce harm when security

incidents happen. Services for security quality management include cyber security audits, promoting best practices, and cyber security drills and exercises. Fig 2. indicate a sharp rise in cyber security issues, which constantly increases with time indexed. In 2021, the data of security incidents handled leads to 1.4 lakhs, wherein the significant contribution is unauthorized network scanning[9] followed by website defacement[10]. The data is transparently raising a concern to map the issue and use the platforms with digital sensitization so that cyberspace can be used positively without fear of cyber hacking intrusions.

Figure 3. Security Alerts Issues by Government (2017-2021)

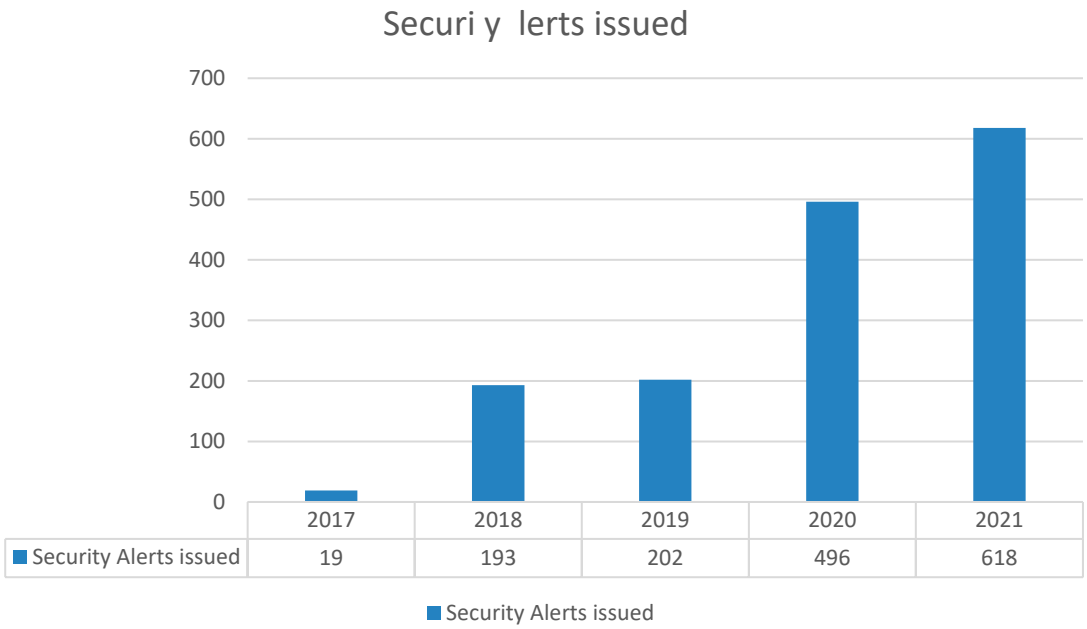


Fig 3. clearly show an increase in security alerts issued by CERT-IN[11] because of the increase in cyber-attacks. In 2017, CERT-IN issued 19 alerts, wherein in 2021, the authority issued 618 alerts, and the significant sharp rise of alerts happened during the pandemic when the major activities shifted to virtual medium. They cater to the requirement against the cyber-attacks; the government has operated the 'Cyber Swachhta Kendra' that helps recognize malicious programs and provides free tools to remove the same.

9 GALTSEV, Aleksey; SUKHOV, Andrei. Network attack detection at flow level. In: Conference on Smart Spaces. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. p. 326-334.

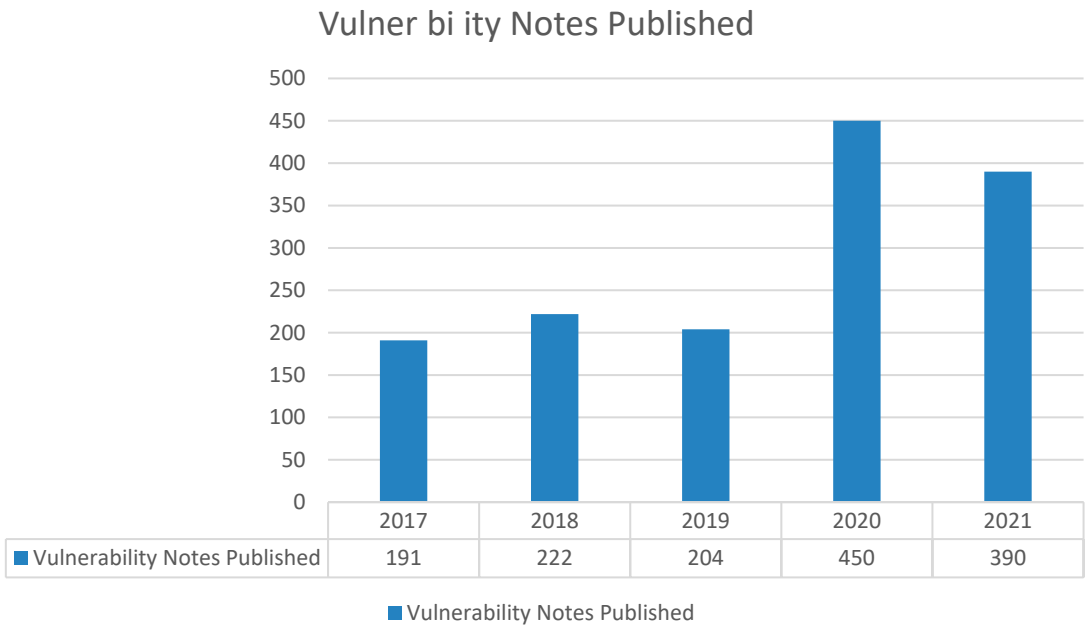
10 ROMAGNA, Marco; VAN DEN HOUT, Niek Jan. Hacktivism and website defacement: motivations, capabilities and potential threats. In: 27th virus bulletin international conference, 2017. p. 1-10.

11 ÍNDIA. Indian Computer Emergency Response Team. Nova Delhi: Ministry of Electronics and Information Technology, [s. d]. Available in: https://www.cert-in.org.in/. Accessed: June, 16, 2022.

Figure 4. Advisories Published by Government (2017-2021)

Fig 4. The CERT-IN published advisories for creating an alert against the malware program against activities like digital payments, etc. The sharp rise of an advisory is in the year 2020 due to pandemic wherein the many activities rise in the virtual medium, and the people are not very accustomed to using these technologies which creates an opportunity to them. The government runs cyber security drills to assist firms in determining how well-prepared they are to fend against cyberattacks. These exercises have greatly aided in enhancing the information infrastructure's cyber security posture, training personnel to handle cyber incidents, and raising awareness of cyber security among the major sector firms.

Figure 5 and 6. Data of Training Organized (2017-2021)



CERT-In routinely organizes pieces of training and workshops to instruct officials of the government, critical sector, public sector industry, and financial & banking sector on a variety of current and targeted themes of cyber security to raise security awareness within these organizations. Fig 5-6. indicate that the CERT-IN organized training to train the experts and to create awareness against these cyber-attacks. In 2018, the finding shows the maximum number of trainings was organized, and in 2020, the least number of training was organized due to the pandemic.

3.2. Laws related to Cyber Crime

In India, cyber-crime is substantially rising, and various contemporary ways are being added to fraud the people. The regulations created to prevent cyber-crime are covered under Information Technology Law, 2000. Cybercrime is there in the virtual forms wherein the perpetrators of an offense are not physically present and are hidden behind the screen doing an algorithm. Tracing these offenders is challenging because the crime mode happens in cyberspace, wherein these offenders use a device or gather information through an unauthorized source. As per Sec. 43[12], unauthorized access by any person into the computer, computer network, or computer system of another[13] wherein the compensation raised to one crore. The sec. 65, which deals with tampering with the computer source documents[14].

12 Information Technology Act, 2008.

13 GOEL, Aaruni; ASHOK, Vasishtha; MANISH, Gupta. In-depth Analysis of an Indian IT Act Related to Unauthorized Access. In: International Journal of Computer Applications, v. 58, n. 7, 2012. Available in: https://www.academia.edu/103515494/In_depth_Analysis_of_an_Indian_I_T_Act_Related_to_Unauthorized_Access?uc-sb-sw=91115826.

14 The offences in respect of computer source documents (codes) are to be kept or maintained by law

Table 1. The table related to the description of cyber crimes

Provision under IT Act, 2000	Description of the provision	Case Laws/ Scams	Description
Section 43	Penalty and Compensation for damage to computer, computer system, etc.	Pune Citibank Mphasis Call Center Fraud Case, 2005[15].	Four call center employees employed by MphasiS in an outsourced facility in India in December 2004 got PINs from four Citi Group customers. These employees could not have obtained the PINs. The call center workers opened new accounts at Indian banks together with others while posing as someone else by using false identities. The Court held that Section 43(a) was applicable here due to the nature of unauthorized access involved in committing transactions.
Section 65	Tampering with Computer Source Documents	Syed Asifuddin and Ors. v. The State of Andhra Pradesh and ors[16].	The electronic 32-bit number encoded into cell phones was manipulated in this case, and Tata Indicom personnel were arrested for manipulation that was only licensed to Reliance Infocomm. The court held that it was tampering with the system code.
Section 66	Computer related offences	A. Shankar vs State Rep. and ors[17]	The petitioner is responsible for information leaks and the broadcast and publication of the material. He also mentioned that Dr. Subramanian Swamy had spoken at a press conference on May 12, 2008, and had given the media access to an audio CD that contained a conversation between the then-Social Welfare Minister, Tmt. Poongothai Aladi Aruna, and Thiru. S. K. Upadhyay, who had been recording all incoming calls on his official telephone.

include knowingly or intentionally (i) concealing; (ii) destroying; (iii) altering; (iv) causing another to conceal; (v) causing another to destroy; (vi) causing another to alter the computer source code.

15 MCKENNA, Brian. Citibank call centre fraud reveals Indian data protection deficit. In: Computer Fraud & Security, v. 4, 2005.

16 2006 (1) ALD Cri 96, 2005 CriLJ 4314.

17 Crl.O.P No.6628 of 2010

Provision under IT Act, 2000	Description of the provision	Case Laws/ Scams	Description
Section 66D	Punishment for cheating by impersonation by using computer resource	Sandeep Vaghese v/s State of Kerala	Sandeep Varghese and eight other people are the subjects of a complaint brought by a representative of a petrochemicals firm for violations of Sections 65, 66, 66A, C, and D of the ITA as Sections 419 and 420 of the IPC. The accused put up a phony website in the firm's name and posted damaging and defamatory information about the company and its directors there. They also sent bogus emails to the bank, suppliers, and customers while posing as the company. Due to the accused's actions, the corporation suffered significant losses.
Section 67	Publication of obscene information in electronic form	Jawaharlal Nehru University MMS scandal case[18]	A pornographic movie was leaked from the JNU campus in 2011. Before posting the video online and even selling it in the blue film market, the two accused initially attempted to extort money from the girl in the video. Sections 292 of the IPC and 66E and 67 of the IT Act were used to charge the defendant in this case.

4 Judicial Responses of Cyber Crime in India

The Manish Kathuria[19] case concerned the stalking of a woman by the name of Ritu Kohli. It was the first known instance of cyber-stalking in India and the impetus behind the 2008 amendment to the IT Act. Following Kohli on a chat platform, Kathuria verbally insulted her before giving out her phone information to other individuals. Later, he started chatting on the website "www.mirc.com" while assuming Kohli's identity. As a result, over three days, she began to get nearly 40 obscene phone calls at strange night hours. This circumstance compelled her to inform the Delhi Police about the incident. Following the complaint filing, the Delhi Police tracked down the IP addresses and detained Kathuria under Indian Penal Code Section 509. Since the IT Act had not yet become effective when the complaint was submitted, it was not used in this case. Although there is no evidence of any further action, this instance alerted Indian legislators to the necessity for laws to deal with cyber-stalking. Even then, Section 66-A was not introduced until 2008. As a result, cases are now being

18 Section 66(E) of Information and Technology Act. | Site Title (wordpress.com) (Last accessed 18.06.2022).

19 C.C. No. 14616/2014

reported under this section of the Indian Penal Code rather than Section 509, as was the case with the Delhi University student who was detained for stalking a woman from Goa by creating fictitious profiles on social networking sites, uploading pictures to them, and claiming she was his wife. It is hoped that the victim will benefit from the decision in this case.

Bazee.com case[20]: The matter was initiated with a CD containing objectionable information being sold on the website in December 2004, and the CEO of Bazee.com was detained. Additionally, Delhi markets were selling the CD. The Delhi Police and the Mumbai City Police sprang into action. Later, bail was paid to free the CEO. The issue of distinguishing between Internet Service Providers and Content Providers was raised as a result. It is the accused's responsibility to prove that he provided the service and not the content. It also raises many questions about how the police should approach cybercrime cases, and extensive education is needed.

Suhas Katti Case[21]: The successful conviction in the Suhas Katti case occurred seven months after the FIR was filed, which is a brief period. The effective handling of the case, which also happened to be the first case of the Chennai Cyber Crime Cell going to trial, deserves a special mention because similar cases have lingered in other states for extended periods. The incident was the publication of an offensive, hurtful, and troublesome comment about a divorcee woman in a Yahoo messaging group. The offender constructed a phony email account in the victim's name and forwarded emails to the victim asking for information. Due to the lady's posting of the message, she received bothersome phone calls from people who mistakenly thought she was soliciting. The accused was convicted under section 469, 509 of IPC, and section 67 of IT act, 2000.

SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra[22]: In India's first instance of cyber defamation, a Delhi court exercised its jurisdiction over a case in which an organization's reputation was being harmed via emails and issued a significant ex-parte injunction. In this case, the defendant Jogesh Kwatra began sending obscene, vulgar, filthy, and abusive emails to his employers and several subsidiaries of the plaintiff company around the world to discredit the business and its managing director, Mr. R K Malhotra. The plaintiff filed a lawsuit seeking a permanent injunction prohibiting the defendant from carrying out his unlawful activities of sending the plaintiff slanderous emails. This order from the Delhi High Court is highly significant because it is the first time an Indian court has been given jurisdiction over a case involving cyber-defamation and has granted an ex-parte injunction prohibiting the defendant from disparaging the plaintiffs by sending them or their subsidiaries offensive, abusive, or defamatory emails.

20 (2008) 105 DRJ 721: (2008) 150 DLT 769

21 C No. 4680 of 2004

22 Original Suit No. 1279 of 2001.

Sony-Sambandh Case: India just had its first conviction for cybercrime. Everything started after Sony India Private Ltd filed a complaint, which operates the website www.sony-sambandh.com and targets Non-Resident Indians. After making an online purchase, the service enables NRIs to mail Sony products to their friends and family in India. She requested that the goods be sent to Arif Azim in Noida and provided her credit card information for payment. The transaction was completed after the credit card company had adequately cleared the money. The company delivered the materials to Arif Azim after doing the necessary due diligence and inspection procedures. The company complained to the Central Bureau of Investigation about internet fraud, and the bureau opened an investigation under Sections 418, 419, and 420 of the Indian Penal Code. Arif Azim was taken into custody after a probe into the situation. Investigations showed that Arif Azim obtained the credit card information of an American citizen while working at a call center in Noida, which he then used fraudulently on the business' website. However, the court believed a liberal stance was necessary because the accused was a young boy (24 years old) and a first-time offender. As a result, the accused was granted a year of probationary release by the court.

5 Conclusion

Botnet Cleaning and Malware Analysis Centre (www.cyberswachhtakendra.gov.in) has been established by CERT compromised devices in India to notify, enable cleaning and securing systems of end users to prevent further malware infections. The center collaborates closely with Internet Service Providers Botnet Cleaning and Malware Analysis Centre Internet Service Providers. Cybercrime, like hacking into computers, can occur through a network system, clicking on strange links, connecting to unsecured Wi-Fi, downloading data and software from dubious sources, consuming energy, emitting electromagnetic radiation, and more. As a growing national concern, cyber security is a serious issue that must be treated.

Modern electronics, including computers, laptops, and cell phones, have built-in firewall security software. However, computers do not always accurately and reliably protect our data. Technology usage requires an upper hand in creating awareness among the users and creating awareness whenever a new bug is reported or any new form of cyber-crime reported; the agency will disseminate the information. Cyber weapons will be deployed more frequently, not less, due to the catastrophic impact they may have on their target information systems and their comparably low costs to traditional kinetic weapons. Since computers and technology will only get better with time, it is essential to clarify the legal ambiguities surrounding cyberwarfare so that nations can comprehend and abide by the norms that will reduce the potential harm these weapons might cause.

CC BY

References

BUSINESS STANDARD. *India registered 136 cybercrime cases every day in 2020: NCRB data*. India, february, 21, 2022. Available in: https://www.business-standard.com/article/current-affairs/india-registered-136-cybercrime-cases-every-day-in-2020-ncrb-data-122022100007_1.html. Accessed june, 10, 2022.

DASHORA, Kamini. Cyber-crime in the society: Problems and preventions. *In: Journal of Alternative Perspectives in the social sciences,* v. 3, n. 1, 2011. p. 240-259.

DATTA, Priyanka et al. A technical review report on cyber crimes in India. *In: 2020 International conference on emerging smart computing and informatics (ESCI). IEEE*, 2020. p. 269-275.

GALTSEV, Aleksey; SUKHOV, Andrei. Network attack detection at flow level. *In: Conference on Smart Spaces*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. p. 326-334.

GOEL, Aaruni; ASHOK, Vasishtha; MANISH, Gupta. In-depth Analysis of an Indian IT Act Related to Unauthorized Access. *In*: *International Journal of Computer Applications*, v. 58, n. 7, 2012. Available in: https://www.academia.edu/103515494/In_depth_Analysis_of_an_Indian_I_T_Act_Related_to_Unauthorized_Access?uc-sb-sw=91115826.

ÍNDIA. *Indian Computer Emergency Response Team*. Nova Delhi: Ministry of Electronics and Information Technology, [*s. d*]. Available in: https://www.cert-in.org.in/. Accessed: June, 16, 2022.

KARALI, Yalcin *et al*. Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India. *In: International Journal of Engineering and Management Research (IJEMR)*, v. 5, n. 2, 2015. p. 43-48.

KUMAR, Vijaya. Growing cyber crimes in India: A survey. *In: 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE). IEEE*, 2016. p. 246-251.

MCKENNA, Brian. Citibank call centre fraud reveals Indian data protection deficit. *In: Computer Fraud & Security*, v. 4, 2005.

MUGWENI, Benison; MUGWENI, Rose. New Patterns in Cyber Crime with the Confluence of IoT and Machine Learning. *In: ICT and Data Sciences. CRC Press*, 2022. p. 117-133.

ROMAGNA, Marco; VAN DEN HOUT, Niek Jan. Hacktivism and website defacement: motivations, capabilities and potential threats. *In: 27th virus bulletin international conference*, 2017. p. 1-10.

UNITED NATIONS. *General Assembly resolution 65/230 and Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8*. Available in: Global Programme on Cybercrime (unodc.org). Accessed: may, 5, 2022.