Educational Administration: Theory and Practice
2024,30(4), 7650- 7654
ISSN:2148-2403
https://kuey.net/

Research Article

Cybersecurity Laws: Protecting Digital Assets And Mitigating Risks

Dr Aniket Deshpande[1*], Radha Kiran[2], James D. Sangma[3], Ashok Ramchandra Panse[4], Dr. Zainab Mirza[5], Sayyad Jilani[6]

[1*]Research Scholar, Sunrise University, Alwar, Rajasthan, Email ID: anik.deshpande@gmail.com
[2]Vice Principal, Department of Political Science, Osmania University, Hyderabad, Telangana, Email ID: airankradha@gmail.com
[3]Research Scholar, Sikkim Professional University, Gangtok, Sikkim, Email ID: ruganokat@gmail.com
[4]Research Scholar, Sikkim Professional University, Gangtok, Sikkim, Email ID: panseashok42@gmail.com
[5]Assistant Professor, Information Technology, M.H. Saboo Siddik COE, Mumbai, Email ID: zainab.mirza@mhssce.ac.in
[6]Professor, M.H. Saboo Siddik College of Engineering, Mumbai, Email ID: jilani.sayyad@gmail.com

Citation: Dr Aniket Deshpande et al. (2024), Cybersecurity Laws: Protecting Digital Assets And Mitigating Risks, *Educational Administration: Theory And Practice*, *30*(4), 7650- 7654, Doi: 10.53555/kuey.v30i4.2624

ARTICLE INFO

ABSTRACT

In the present era, it is widely recognized that a majority of activities are commonly conducted on the internet, ranging from online business transactions to financial exchanges. Today, the entire nation is transitioning to the era of digitization and networking, which undoubtedly brings organized benefits to different industries such as e-commerce, communication, and more. Given the global nature of the internet, individuals have the ability to access online information from any location. A small minority of individuals have been utilizing internet technology for illicit activities such as unlawful intrusion into others' networks and engaging in frauds. In the context of the internet, the term "cybercrime" refers to any illegal behaviors or offenses that are done online. This is the only way to overcome this challenge. In an effort to discourage and punish those who violate computer laws, the phrase "Cyber Law" was coined. When it comes to the legal framework that governs the Internet, cyberspace, and other legal problems, cyber law is the subject of discussion. It covers a wide range of topics, such as the right to free speech, access to and utilization of the internet, personal privacy and security online, and internet access. To provide a more particular definition, it is generally known as the law of the internet.

Keywords: *Cybercrime, Internet, Cyber law, Unauthorized access, Cyberspace, Punish, Network*

Introduction

The advent of computers has significantly facilitated human existence, being utilized for a wide range of applications, from individual use to large-scale implementation in global organizations. Computer can be defined as a machine capable of storing and manipulating information or instructions provided by the user. For many years, computer users have been using computers for objectives that are either self-serving or beneficial to others, but are incorrect or misguided. Thus, "Cybercrime" emerged as a result of this. This has resulted in the participation in actions that are deemed criminal by society. Cybercrime refers to criminal activities that are carried out utilizing computers or computer networks, primarily over the internet[1]. The term "Cyber Law" is now introduced. While lacking a precise definition, we can broadly describe it as the legal framework that regulates activities in the digital realm known as cyberspace. Cyber laws pertain to the legal regulations that govern the realm of cyberspace. The field of Cyber Law encompasses various aspects such as cybercrimes, digital and electronic signatures, data protection, and privacy. The first IT Act[2] of India, which

[1] "Animesh Sarmah, Roshmi Sarmah , Amlan Jyoti Baruah, A brief study on Cyber Crime and Cyber Law's of India, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 06 | June - 2017 https://www.southcalcuttalawcollege.ac.in/Notice/50446IRJET-V4I6303.pdf (Retrieved January 5, 2024)

[2] THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000)

was approved by the UN's General Assembly, was based on the "United Nations Model Law on Electronic Commerce[3]" (UNCITRAL) Model[4].

Cyber Crime

The term "Cybercrime" was initially coined by Sussman and Heuston[5] in 1995. Cybercrime cannot be encapsulated by a singular definition; rather, it is more accurately characterized as an assemblage of several acts or behaviors. These activities are based on the concrete criminal item that affects computer data or systems. These are the unlawful behaviors in which a digital device or information system is used as a tool, target, or both at the same time. Cybercrime, often known as electronic crimes, computer-related crimes, e-crime, high technology crime, or information age crime, involves a variety of unlawful behaviors carried out using digital methods.

Cybercrime refers to offenses or criminal activities that occur through electronic communications or information systems. These offenses encompass unlawful conduct that involve the use of a computer and a network. As the internet continues to advance, cybercrime activities are also on the rise. This is because criminals may now commit crimes without needing to be physically present. Cybercrime is distinct in that the victim and the perpetrator may never have any direct interaction. Cybercriminals frequently choose to operate from nations that have either non-existent or weak cybercrime legislation to minimize the likelihood of being detected and prosecuted.[6]

Cyber Law

Cyber Law emerged to regulate and address criminal activities conducted via “the internet, cyberspace, or computer resources”. Cyber Law refers to the legal difficulties that arise from the use of communication or computer technology. It is crucial as it pertains to nearly all facets of activities and transactions that occur either on the internet or other communication devices. Every activity & reaction in Cyberspace, whether we are conscious of it or not, is subject to legal and Cyber legal perspectives[7].

Authorities and regulatory agencies have acknowledged the significance of safeguarding personal data and have implemented several rules and regulations to defend the privacy rights of individuals. An exemplary instance is the “General Data Protection Regulation[8] (GDPR)” of the European Union, which enforces stringent protocols around the gathering, handling, “and retention of data, thereby empowering individuals with increased control over their personal information. Adhering to these regulatory frameworks is essential for enterprises to safeguard the personal data they handle and to prevent significant penalties and legal consequences.[9]

Financial security has become a crucial element of contemporary cyber security procedures. The continuous process of converting traditional systems into digital ones, along with the growing acceptance of financial services provided through the internet, have generated multiple prospects for expansion and advancement. Consequently, ensuring financial security has become an essential component of cyber security, necessitating strong methods and strategies to protect financial data, services, and infrastructure[10].

The Information Technology Act of India[11], 2000

The Information Technology Act[12], 2000 (often referred to as ITA-2000 or the IT Act) is a legislation enacted by the Indian Parliament (No. 21 of 2000) and officially announced on October 17, 2000, as stated by

---

[3] UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998

[4] Mittal, Rahul. “IMPACT OF SOCIAL MEDIA ON SOCIETY & CYBERLAW.” A. K. Publications 1, no. 1 (2014): 242–51. (Retrieved January 5, 2024)

[5] Sandip Naik, S., & Patil, D. (n.d.). CYBER CRIME AND CYBER LAW’S OF INDIA. Retrieved January 6, 2024, from www.irjmets.com (Retrieved January 6, 2024)

[6] Phillips, K. ;, Davidson, J. C. ;, Farr, R. R. ;, Burkhardt, C. ;, Caneppele, S. ;, Aiken, M. P., Dinis-Oliveira, F., Alves, C., Barone, P. M., Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P.” “(2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences 2022, Vol. 2, Pages 379-398, 2(2), 379–398. https://doi.org/10.3390/FORENSICSCI2020028 (Retrieved January 6, 2024)

[7] Chhabra, Gunjan & Chhabra, Kanika. (2014). A Study on Emerging Issue on Cyber Law. 10.13140/RG.2.1.3007.8568. (Retrieved January 5, 2024)

[8] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

[9] Bharat Bhushan, The Growing Importance of Cyber Security in the Digital Age, INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD, Volume - 9, Issue - 5, May - 2023. DOIs:10.2015/IJIRMF/202305031 https://www.ijirmf.com/wp-content/uploads/IJIRMF202305031-min.pdf (Retrieved January 5, 2024)

[10] ibid

[11] Ibid”

[12] “ibid

Wikipedia. The most significant legislation in India pertaining to digital crimes, cybercrimes, and electronic trade is the primary focus. The basis of this is the United Nations Model Law on Electronic Commerce[13] 1996 (UNCITRAL Model), which was suggested by the General Assembly of the United Nations through a resolution on 30 January 1997.[14]

Recent Cases

Shreya Singhal v. Union of India[15] (2013)

Here, the Supreme Court kept a close eye on the case as it examined the constitutionality of Section 66A[16] of the IT Act. Following the death of a political trailblazer in Mumbai, two women were apprehended under Section 66A[17] of the IT Act for allegedly making defamatory and threatening comments on Facebook. The women have taken legal action in response to the recorded conversation by requesting a review of the validity of Section 66A[18] of the IT Follow up, arguing that it infringes upon their right to free expression. Anyway, the Court also noted that the IT Act's Section 66A does not violate Article 14[19] of the Indian Constitution since there was a clear difference between data transmitted through the web and other forms of conversation. The standard of procedural preposterousness was also left unanswered by the Apex Court, which is surprising given that it is clearly unconstitutional.

CBI v. Arif Azim[20] (Sony Sambandh case)

After making an online payment, non-resident Indians could send Sony products to their loved ones in India through a website named www.sony-sambandh.com. Someone logged onto the site in May 2002 using the identity of Barbara Campa and asked for a Sony Shading TV and a cordless phone for Arif Azim of Noida. Arif Azim was notified of her request when she paid with her credit card. However, since the actual owner denied making such a purchase, the charge card company notified the business that the payment was unapproved. A case was registered under Areas 418[21], 419[22], and 420[23] of the Indian Reformatory Code, 1860, and a protest was put up with the CBI along similar lines. After a year of post-trial proceedings, the court handed over the indicted individual. This case was a watershed moment in the history of digital law because it proved that when the IT Act[24] falls short, the Indian Reformatory Code[25], 1860 can step in as a strong alternative.

Digital Assault on COSMOS Bank

As a result of a shocking cyberattack in August 2018, the Pune branch of Universe Bank lost Rs 94 crores. The thieves might have sent the funds to a Hong Kong bank if they had gained access to the main server. Along with this, the hackers breached the ATM server and stole details from many Rupay and VISA pay cards. The user's text is a single period. As a result of a breach in the exchange system, such as the connection between the integrated system and the payment channel, both the bank and the record holders were not notified about the funds transfer. Based on the global cybercrime investigation, a total of 450 credit cards were utilized in about 14,000 transactions that were spread out over 28 different nations. Approximately 2,800 transactions were carried out using 400 cards. It was unique, and to be honest, the first malware attack of its kind to completely disable communication between the bank and the payment gateway.

Meghana Bhatt v/s. The State[26], 23rd April 2019

Concerning the alleged violation of Section 506[27] of the Indian Penal Code, the case involving the second respondent is that on (10-05-2016), the applicant had previously communicated with him, agreeing not to marry anyone other than the solicitor. Their prior claim in the question—that they were head over heels for one other until 10-07-2016—is cast in doubt by this allegation. Beyond that, it doesn't matter if the applicant's claim of such a threat is true or not; what matters is that the solicitor was planning to marry the later respondent on that day and didn't want him to marry someone else. Therefore, the alleged threat cannot be shown as a

---

[13] ibid
[14] Dunn, M. H., & Valeriano, B. (2018). Cybersecurity: How national and international politics affect digital security. In Routledge Handbook of Global Security Policy. (Retrieved January 5, 2024)
[15] Shreya Singhal v. Union of India (2013) 12 SCC 73
[16] Section 66A of THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000)
[17] ibid
[18] ibid
[19] Article 14. The Constitution of India, 1950.
[20] CBI v. Arif Azim (Sony Sambandh case)"
[21] "Sec 418, Indian Penal Code 1860, Act No. 45 of 1860.
[22] Sec 419, Indian Penal Code 1860, Act No. 45 of 1860.
[23] Sec 420, Indian Penal Code 1860, Act No. 45 of 1860.
[24] ibid
[25] Indian Penal Code 1860, Act No. 45 of 1860.
[26] Meghana Bhatt v/s. The State, 23rd April 2019
[27] Sec 506, Indian Penal Code 1860, Act No. 45 of 1860.

violation of section 506[28] of the Indian Penal Code. There was insufficient evidence in the first information report (FIR) to establish guilt under Section 503 of the Indian Penal Code, and hence, no guilt under Section 506 either.

SMC Pneumatics (India) Pvt. Ltd. v Jogesh Kwatra[29] (2016)

In this scenario, Litigant Jogesh Kwatra served as a representative of the plaintiff's organization. He initiated the act of transmitting offensive, derogatory, obscene, detrimental, and defiled messages to his superiors and to numerous subordinates of the mentioned organization worldwide, with the intention of criticizing the organization and its Chief Executive Officer, Mr. R K Malhotra. During the exams, it was noted that the email originated from a Digital Bistro located in New Delhi. The cybercafe expert identified the respondent during the investigation. On May 11, 2011, the plaintiff terminated Litigant from their services. The court imposed restrictions on the litigant, prohibiting them from disseminating or publishing any defamatory or oppressive information about the plaintiffs on the internet.

Conclusion

The prevalence of digital offenses against women in India is increasing rapidly, resulting in significant societal repercussions. Every internet user is constantly at risk of becoming a victim of cybercrime. Our country is among the few nations that have implemented the IT Act, 2000 to safeguard our nation from cybercrimes. However, this legislation lacks specific provisions to protect women and children from the digital realm. Therefore, the mere establishment of laws in the country would not be sufficient cause for a complete crackdown on these offenses. To effectively combat these crimes in society, we as individuals must take specific actions to prevent harm to women and other vulnerable groups in the nation.

In order to protect themselves against online harassment targeting women, it is advisable for them to refrain from engaging in conversations with unfamiliar individuals. Individuals on the other side of the computer may not be who they claim to be. Individuals should strive to safeguard their passwords and avoid storing sensitive information on their computer, as it can be accessed by hackers. If anything looks to be unusual or incorrect, promptly call police enforcement.

The internet poses significant challenges in terms of governance, leading to certain activities falling into a legal gray area where there is a lack of regulatory framework. Consequently, there is still a long way to go before implementing a comprehensive and robust legislation for cybercrimes in India.

References

Articles

1. Animesh Sarmah, Roshmi Sarmah , Amlan Jyoti Baruah, A brief study on Cyber Crime and Cyber Law's of India, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 06 | June -2017 https://www.southcalcuttalawcollege.ac.in/Notice/50446IRJET-V4I6303.pdf (Retrieved January 5, 2024)
2. Mittal, Rahul. "IMPACT OF SOCIAL MEDIA ON SOCIETY & CYBERLAW." A. K. Publications 1, no. 1 (2014): 242–51. (Retrieved January 5, 2024)
3. Chhabra, Gunjan & Chhabra, Kanika. (2014). A Study on Emerging Issue on Cyber Law. 10.13140/RG.2.1.3007.8568. (Retrieved January 5, 2024)
4. Bharat Bhushan, The Growing Importance of Cyber Security in the Digital Age, INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD, Volume - 9, Issue - 5, May - 2023. DOIs:10.2015/IJIRMF/202305031 https://www.ijirmf.com/wp-content/uploads/IJIRMF202305031-min.pdf (Retrieved January 5, 2024)
5. Dunn, M. H., & Valeriano, B. (2018). Cybersecurity: How national and international politics affect digital security. In Routledge Handbook of Global Security Policy. (Retrieved January 5, 2024)
6. Sandip Naik, S., & Patil, D. (n.d.). CYBER CRIME AND CYBER LAW'S OF INDIA. (Retrieved January 6, 2024, from www.irjmets.com)
7. Phillips, K. ;, Davidson, J. C. ;, Farr, R. R. ;, Burkhardt, C. ;, Caneppele, S. ;, Aiken, M. P., Dinis-Oliveira, F., Alves, C., Barone, P. M., Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions," Typologies and Taxonomies. Forensic Sciences 2022, Vol. 2, Pages 379-398, 2(2), 379–398. https://doi.org/10.3390/FORENSICSCI2020028 (Retrieved January 6, 2024)

Cases

1. Shreya Singhal v. Union of India (2013) 12 SCC 73
2. CBI v. Arif Azim (Sony Sambandh case)

[28] Ibid"

[29] "SMC Pneumatics (India) Pvt. Ltd. versus Jogesh Kwatra CM APPL. No. 33474 of (2016)"

3. Meghana Bhatt v/s. The State, 23rd April 2019
4. SMC Pneumatics (India) Pvt. Ltd. versus Jogesh Kwatra CM APPL. No. 33474 of (2016)

Laws and statues

5. THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000)
6. UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998
7. EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016
8. Section 66A of THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000)
9. Article 14. The Constitution of India, 1950.
10. Sec 418, Indian Penal Code 1860, Act No. 45 of 1860.
11. Sec 419, Indian Penal Code 1860, Act No. 45 of 1860.
12. Sec 420, Indian Penal Code 1860, Act No. 45 of 1860.
13. Sec 506, Indian Penal Code 1860, Act No. 45 of 1860.