Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
July-December 2023 4(2), 1747–1751

PRIVACY RIGHTS IN THE AGE OF CYBERCRIME: A CRIMINAL LAW PERSPECTIVE

Dr. Ashwani Kumar Gupta[1]

[1] LL.M., Ph.D., Principal, T.R.C. Law College, Vasudev Nagar, Satrikh, Barabanki

ABSTRACT

The rapid advancement of technology in the digital age has transformed how individuals interact, communicate, and conduct business online, but it has also given rise to significant challenges regarding the protection of privacy rights. Data breaches, hacking, identity theft, and cyberstalking are just a few examples of the many forms of cybercrime that affect people's right to privacy and the protection of their private information. Looking at cybercrime from a criminal law standpoint, this abstract explores the increasing conflict between private rights and the prevalence of the crime. Cybercriminals take advantage of the internet's anonymity and worldwide reach, making it difficult to enforce privacy regulations in the digital world. Cybercrime presents unique issues that current legal frameworks are ill-equipped to handle; this paper argues that this calls for new laws, more robust cybersecurity measures, and more international cooperation. The significance of developing criminal laws to defend people' rights against cybercrime is highlighted by the core issue of striking a balance between protecting privacy and guaranteeing security in an ever more interconnected world.

Keywords: Privacy Rights, Cybercrime, Data Protection, Identity Theft, Digital Privacy

DOI
10.29121/shodhkosh.v4.i2.2023.2920

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

1. INTRODUCTION

The rapid growth of the digital age has transformed how people live, work, and communicate. At the heart of this transformation lies the widespread exchange of data, often with minimal regard for its protection. With personal information now regularly shared and stored online, the concept of privacy has become increasingly vulnerable. While technological advancements offer numerous benefits, they also expose individuals, corporations, and even governments to a new breed of threats: cybercrime. Cybercriminals exploit the digital landscape to steal, manipulate, and misuse sensitive data, creating an environment where privacy rights are constantly at risk. The intersection of privacy rights and cybercrime raises fundamental legal, ethical, and societal concerns, as it challenges the balance between protecting personal freedoms and ensuring security in an increasingly interconnected world.

Privacy rights have long been considered a fundamental pillar of individual autonomy and dignity. Historically, the right to privacy was enshrined in legal systems as a safeguard against the government's overreach and as a means of protecting personal boundaries from external intrusion. The advent of the internet, however, has drastically reshaped the concept of privacy. The digital age has brought about a vast proliferation of personal data, collected by both public and private institutions for various purposes such as marketing, social networking, and even governmental surveillance. With this increase in data generation comes the corresponding rise in the risk of cybercrime, where malicious actors seek to exploit weaknesses in digital security for fraudulent or harmful purposes.

How to cite this article (APA): Gupta, A.K. (2023). Privacy Rights in the Age of Cybercrime: A Criminal Law Perspective. *ShodhKosh: Journal of Visual and Performing Arts, 4*(2), 1747–1751. doi: 10.29121/shodhkosh.v4.i2.2023.2920

When considering violations of privacy rights, the term "cybercrime" encompasses a broad spectrum of actions, including but not limited to: hacking, cyberstalking, identity theft, and data breaches. Financial loss, reputational injury, mental distress, and even physical risk may result from these crimes, which erode people' capacity to manage their personal information. Cybercriminals often operate from multiple countries due to the worldwide nature of the internet, which makes it difficult for law enforcement to successfully monitor and punish them. It is already difficult to safeguard personal information online due to the intricacy of cybercrime and the anonymity it offers. As an example, advanced hacking methods may steal sensitive information from unwary people or businesses, sometimes without their awareness or agreement. Because of this, people's right to privacy is being violated at an alarming rate, and they have little tools to fight back.

The challenges posed by cybercrime to privacy rights are not merely technological; they also raise profound questions about the relationship between security and individual freedoms. Governments, in an effort to combat cybercrime, often propose and enact laws that grant sweeping surveillance powers to law enforcement agencies. While these measures are intended to protect citizens from cybercriminal activity, they can also encroach upon individuals' privacy rights. Laws that require companies to store and share user data, or policies that enable mass surveillance, often ignite debates about the erosion of privacy in the name of security. The tension between security measures and privacy protections is one of the most contentious issues in the current legal and political landscape, as the question arises: how much privacy are individuals willing to sacrifice for the sake of safety, and where should the line be drawn?The relationship between privacy rights and cybercrime also highlights the need for stronger consumer protection and greater digital literacy. As the risks associated with cybercrime continue to evolve, individuals must be equipped with the knowledge and tools to protect their personal information online. Knowledge of phishing attempts, the significance of using complex passwords, and methods for securing devices and networks are all part of this. Everyone from governments to corporations to civil society groups has a role to play in raising people's privacy awareness and protecting them from cybercriminals.

2. FORMS OF CYBERCRIME IMPACTING PRIVACY

Cybercrime comes in various forms, each with unique implications for privacy. The following are some key types:

HACKING AND UNAUTHORIZED ACCESS

In order to steal sensitive information, hackers gain illegal access to computer systems, networks, or devices. Hackers get past security measures by taking advantage of loopholes in the system or by manipulating users via social engineering. Notable incidents like Yahoo's 2013 data breach made headlines because it compromised the accounts of billions of users and disclosed sensitive information including passwords, security questions, and email addresses.

IDENTITY THEFT

Cybercriminals commit identity theft when they acquire sensitive information about their victims, such as their social security numbers, credit card data, or login passwords, and use it to commit impersonation crimes. Theft, low credit ratings, and mental anguish are all possible outcomes of such abuse. The digitalization of personal data has contributed to a 113% increase in identity theft cases between 2019 and 2020, according to the U.S. Federal Trade Commission.

PHISHING AND SOCIAL ENGINEERING

Phishing is the practice of using misleading electronic communication channels (email, text, website) to acquire sensitive information. Hackers steal sensitive information, such bank account numbers or company login passwords, by taking advantage of people's trust and curiosity. Massive data breaches impacting millions of people are a common outcome of successful phishing efforts.

RANSOMWARE ATTACKS

The data of victims is encrypted by ransomware and cannot be accessed unless a ransom is paid. In addition to interfering with operations, these assaults compromise privacy by making sensitive data public. Critical infrastructure is particularly susceptible to attacks like the one that hit the Colonial Pipeline in 2021.

DATA BREACHES AND CORPORATE ESPIONAGE

Data breaches occur when cybercriminals infiltrate organizations to steal or expose stored information. Companies like Target, Equifax, and Facebook have faced significant breaches, compromising customer data and eroding trust. Corporate espionage further amplifies these risks, as competitors or state actors target trade secrets and strategic information.

3. CONSEQUENCES OF CYBERCRIME ON PRIVACY

The impact of cybercrime on privacy extends beyond individuals to institutions and society at large. Its consequences can be classified into direct and indirect effects.

FINANCIAL LOSSES

Businesses and people alike might lose a lot of money due to cybercrime. Unauthorized purchases or fraudulent loans may befall victims of identity theft, and organizations may have to pay to repair trust, compensate victims, and reduce the impact of breaches. Forecasts indicate that by 2025, the yearly cost of cybercrime would exceed $10.5 trillion on a worldwide scale.

EMOTIONAL AND PSYCHOLOGICAL EFFECTS

Privacy breaches caused by cybercrime can lead to emotional distress, anxiety, and a loss of trust. Victims of cyberbullying or online harassment may suffer from depression and social withdrawal. The intrusive nature of cybercrime undermines the sense of security associated with personal information.

REPUTATIONAL DAMAGE

For organizations, data breaches can damage reputation and customer loyalty. Companies like Facebook and Equifax have faced public backlash and legal actions due to their inability to protect user data. On an individual level, leaked personal information can result in public humiliation or career setbacks.

4. KEY LAWS GOVERNING PRIVACY IN CYBERSPACE IN INDIA

India's legal system addresses privacy and cyberspace through a combination of constitutional guarantees, statutory provisions, and regulatory frameworks:

THE INFORMATION TECHNOLOGY (IT) ACT, 2000

Cyberspace in India is primarily governed under the IT Act. Important privacy-related provisions comprise:
Section 43A: Obligates companies to implement reasonable security practices for sensitive personal data.
Section 72: Penalizes unauthorized disclosure of personal information.
Section 66E: Criminalizes capturing, publishing, or transmitting private images without consent.

THE PERSONAL DATA PROTECTION BILL (PDPB)

The PDPB, which is anticipated to become law soon, aims to provide comprehensive protection for personal data, aligning with global standards like the GDPR. It establishes:
Rights for individuals regarding data access, correction, and erasure.
Obligations for data processors and controllers.
A regulatory authority to enforce compliance.
Indian Penal Code (IPC), 1860 Various IPC provisions address offenses like identity theft, defamation, and criminal intimidation, which intersect with privacy violations in cyberspace.
Aadhaar Act, 2016 While facilitating digital identity verification, the Act includes privacy safeguards, such as restrictions on data sharing and penalties for misuse of Aadhaar information.
Telecom Regulatory Authority of India (TRAI) GuidelinesTRAI governs the use of personal data by telecom operators, emphasizing user consent and protection against spam and unauthorized surveillance.

5. POTENTIAL IMPROVEMENTS AND SOLUTIONS

What keeps aggravating the cyber-criminal environment is the fact that numerous web-based threats require cross-sectional response aimed at eradicating such vulnerabilities and bolstering cybersecurity resilience. It is the aim of this paragraph provide presents cognitive equilibrium through the legal provision, advice to the policy and improve the cybersecurity.

LEGISLATIVE_PROPOSALS

It is through legislation that we tackle the problem of cybercrime with a precise legal mechanism. One of the things that call for consideration is to come up with several deliberative processes to enable us tackle the emerging cyber threats. To curb cybercrime and increase penalties for responsible cybergangs, it would be necessary to update and revise existing legislation, such as the Indian Penal Code (IPC) and the Information Technology Act [1]. To address the lack of legislation and establish new standards for the prosecution of cybercrime using emerging technologies, lawmakers should implement new laws tailored to emerging technologies like blockchain, artificial intelligence (AI), and the Internet of Things (IoT) [2]. Moreover, establishing cooperation mechanisms at international level and extradition agreements aimed at facilitating the extradition of cyber-criminals from other countries to the place where crime was committed is an obvious way to strengthen law-enforcement fighting cyber offenses [3].

POLICY RECOMMENDATIONS

Policy making plays an essential role for enabling a community that will encourage the cybersecurity implementation. The primary key is to develop a national cybersecurity framework, which requires the presence of proactive measures, risk management structure as well as capacity-building programs to build up the national cybersecurity preparedness. Also, cooperation with private-public partnershipto achieve info sharing, threat intelligence sharing and coordinated cybersecurity operations can be a powerful tool for critical infrastructure protection and in cyber threat prevention [6]. Moreover, educating and making people cybersecurity aware and digital literate through campaigns, training programs, and community outreach helps users to become proactive and apply security practices that will protect their personal and organizational information from cyber risks.

ENHANCING CYBERSECURITY MEASURES

The set-up of all-inclusive and up-to-date cybersecurity tools is integral for the impediment of vulnerabilities and prevention of cyberattacks. By establishing powerful cyber security system grounded on NIST Cybersecurity Framework, organizations will be able to follow a certain flow to provide identification, detection, protection, response and recovery services in case of cyber events. Besides, investors in frontier technologies like AI, ML also enhance cybersecurity by preventing such actions, rapid response, and data security [8]. Also, tight regulations of compliance rules having same rules that apply to all sectors would pull and possibly to encourage companies to take cybersecurity as seriously and to invest in their cyber defense mechanisms effectively [9].By means of holistic approach and integration of legislative, policy and technical efforts, the situation of the cybersecurity resilience in the midst of stakeholders can become better and cyber threats can be minimal.

LOSS OF AUTONOMY

Privacy is closely tied to personal autonomy. When cybercriminals exploit private data, they undermine individuals' ability to control their information. Surveillance and tracking through malware or spyware further erode autonomy, creating an environment of distrust and fear.

NATIONAL SECURITY RISKS

Cybercrime targeting government agencies, defense systems, or critical infrastructure poses risks to national security. Espionage, sabotage, or ransomware attacks can expose sensitive information, disrupt services, and jeopardize the safety of citizens.

6. CONCLUSION

One of the biggest problems with the internet age is the way privacy rights and criminality interact with one other. Protecting one's privacy from the ubiquitous dangers offered by cybercriminals has become more challenging as technology keeps evolving at a dizzying rate. Identity theft, data breaches, and monitoring are just a few examples of the many privacy violations made possible by the internet's borderless and anonymous nature. It is essential to fight cybercrime with stricter laws and better security measures, but we must also ensure people's basic right to privacy. There are difficulties between privacy and safety when government actions to provide security intrude upon human liberties, making it difficult to strike a balance between the two. Furthermore, new threats are introduced by the fast proliferation of technologies such as the Internet of Things, cloud computing, and artificial intelligence, making it even more difficult to secure privacy in the digital age. In order to tackle these concerns head-on, we need to work together to improve regulatory frameworks, boost international collaboration, and provide people the information and tools they need to keep their personal data safe. Ensuring people may confidently, securely, and autonomously explore the digital environment requires that privacy rights remain important to discussions about cybersecurity and criminality.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Navyasree, Soma & Prakash, Febin. (2024). UNDERSTANDING THE CYBER LAW IN THE AGE OF CYBER CRIME: A REVIEW. 58. 199-212.

Malik, Jitender & Choudhury, Sanjaya. (2019). Privacy and surveillance: The Law relating to Cyber Crimes in India. Journal of Engineering, Computing and Architecture. 9. 74-98.

Ashikur, Md & Tareq, Rahaman & Islam, Md. (2024). The Major Role of Cyber Law in Ensuring Privacy of Netizens: A Case Study of Bangladesh Perspective. International Journal of Research and Scientific Innovation. XI. 219-227.

Ruddin, Isra & SGN, Subhan. (2024). Evolution of Cybercrime Law in Legal Development in the Digital World. JurnalMultidisiplin Madani. 4. 168-173. 10.55927/mudima.v4i1.7962.

Mohsin, Kamshad. (2020). Global Perspective of Cyber Crimes and Related Laws. SSRN Electronic Journal. 10.2139/ssrn.3673938.

Batrachenko, Tetiana & Lehan, Iryna &Kuchmenko, Vitalii & Kovalchuk, Volodymyr &Mazurenko, Olha. (2024). Cybercrime in the context of the digital age: analysis of threats, legal challenges and strategies. Multidisciplinary Science Journal. 6. 2024ss0212. 10.31893/multiscience.2024ss0212.

Syahril, Muh. Akbar. (2023). Cyber Crime in terms of the Human Rights Perspective. International Journal of Multicultural and Multireligious Understanding. 10. 119. 10.18415/ijmmu.v10i5.4611.

Shah, Naseeb Ur Rehman. (2013). Law and Society in the Digital Age: A Study of Cyber Law Theories and Comparative Legal Mechanisms. 10.13140/RG.2.2.20500.31366.

Holt, Thomas & Bossler, Adam & Seigfried-Spellar, Kathryn. (2017). Law Enforcement, Privacy, and Security in Dealing with Cybercrime. 10.4324/9781315296975-2.

Chhabra, Gunjan & Chhabra, Kanika. (2014). A Study on Emerging Issue on Cyber Law. 10.13140/RG.2.1.3007.8568.

Amoo, Olukunle&Atadoga, Akoh& Abrahams, Temitayo &Farayola, Oluwatoyin &Osasona, Femi & Ayinla, Benjamin. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews. 21. 205-217. 10.30574/wjarr.2024.21.2.0438.

Sarkar, Banhita& Mitra, Anirban & Chatterjee, Sujoy. (2023). Cybercrime and Cybersecurity Laws in Current and Future Contexts With Evolving Crimes Across National Boundaries. 10.4018/978-1-6684-8422-7.ch014.

Atrey, Ishan. (2023). Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. 10. 183-197. 10.1729/Journal.35277.