



## Cyber crime against women in India-A critical analysis

Dr. B Vijayalaxmi

Professor, Department of Law, Osmania University, Hyderabad, Telangana, India

### Abstract

Cybercrime against women in India has emerged as a serious threat with the growing digitalization of society. Women face various forms of online abuse, including cyberstalking, harassment, morphing, and revenge pornography, which violate their dignity and safety. This paper critically analyzes the nature, causes, and patterns of cybercrimes targeting women, evaluates the effectiveness of legal frameworks such as the IT Act, 2000 and IPC provisions, and examines judicial responses. It also discusses social and technological challenges in addressing such crimes and offers policy suggestions for enhanced digital safety, legal reform, and awareness to ensure gender-sensitive cyberspace governance.

**Keywords:** Cybercrime, women, online harassment, information technology act, digital safety

### Introduction

Cybercrime, a crime involving technology, has a history dating back to the 18th century. The earliest recorded cyberattack occurred in France in 1834. The internet and World Wide Web have increased public awareness and usage, impacting the landscape of cybercrime. Technology offers advantages like research, knowledge exploration, and instant communication, but it is susceptible to misuse. The intentional misuse of technology contributes to the daily increase in cybercrime, which is a growing concern. The dual nature of technology and its potential drawbacks make it a complex issue.

### Classifying Cybercrimes

Cybercrimes are offenses committed using technology, often involving the role of a computer in the offense. Computers can be the direct target of the crime, serve as tools for traditional crimes, or be used for malicious software to destroy digital information. Internet crimes can be categorized into three main groups: individuals who gain unauthorized access but stop, those who continue to commit traditional crimes, and those who use viruses, Trojan horses, or logic bombs to destroy digital information.

World Wide Web crimes involve traditional offenses facilitated by the web, such as cheating and fraud. Email crimes involve threats, extortion, cyberstalking, email bombing, defamation, fraud, and the launching of malicious programs. Usenet newsgroups and Internet Relay Chat (IRC) also serve as platforms for illicit activities. Interpol categorizes cybercrimes into six broad groups: unauthorized access or interception, alteration of computer data, and computer-related frauds. Classifications can be made based on the computer's role or the victim affected. Victim-based classifications include crimes affecting individuals, national security, and the economy. Cybercrimes can also be categorized by their content or the persons involved, distinguishing between crimes committed by insiders versus outsiders.

### Cybercrimes Against Women

The landscape of crime, much like society itself, is constantly evolving. While acts of harassment, abuse, and

violence against women are tragically not new phenomena, the digital age has introduced a complex and pervasive extension of these harms: cybercrimes against women. Often viewed as a modern form of victimization, these crimes leverage technology to inflict psychological, emotional, and sometimes physical distress, highlighting how offline gender inequalities are amplified and perpetuated in online spaces (European Parliament, n.d.). This essay will delve into the underlying causes that make women disproportionately vulnerable to digital aggression, explore the various forms these cybercrimes take, and examine the legal frameworks in India and internationally that seek to offer protection and justice.

### Understanding Vulnerability: Why Women Become Targets

The causes of cybercrime against women are deeply rooted in societal structures and patriarchal norms, mirroring the power imbalances that exist in the physical world. It's often observed that women are, unfortunately, perceived as more susceptible targets, a perception that digital platforms can exploit. One contributing factor is the persistent societal view that women are often seen as "prey", a deeply troubling notion that translates into online spaces where anonymity can embolden perpetrators. This perception stems from entrenched gender biases and a culture that, in many instances, fails to adequately address the root causes of gender-based violence (European Parliament, n.d.). Online, this manifests as a sense of entitlement from aggressors, who may feel justified in harassing, objectifying, or controlling women without immediate physical repercussions.

Furthermore, it is often argued that women can be "easy to be trapped" through various social engineering tactics (CyberTalents, n.d.). Cybercriminals exploit human vulnerabilities, such as trust, empathy, or the desire for connection. Women, perhaps more frequently exposed to social engineering scams or online grooming tactics, might be more susceptible to deceptive schemes that ultimately lead to their exploitation or victimization (Jogulamba Gadwal Police, n.d.). This is not a reflection of inherent weakness, but rather a consequence of sophisticated manipulation techniques employed by perpetrators.

Economic disparities also play a significant role; when women are economically weak, they might be more vulnerable to financial scams, phishing attempts, or blackmail (GeeksforGeeks, n.d.). The promise of quick money or a better life can be a powerful lure, exploited by criminals to gain access to personal information or financial resources, leading to severe economic and emotional distress. This economic vulnerability can also limit their access to resources needed for digital literacy, protection, or legal redress.

Perhaps one of the most heartbreaking realities is that women are more often victimized by a known person rather than an unknown individual (GeeksforGeeks, n.d.). This highlights the insidious nature of intimate partner violence (IPV) and crimes committed by acquaintances, where pre-existing trust and access to personal information are leveraged for digital abuse. Former partners, disgruntled friends, or even family members can exploit intimate knowledge to harass, defame, or blackmail, making the betrayal even more profound and difficult to address. The emotional toll of such betrayal often far outweighs the technical aspects of the crime.

### **Digital Shadows**

The landscape of crime, much like society itself, is constantly evolving. While acts of harassment, abuse, and violence against women are tragically not new phenomena, the digital age has introduced a complex and pervasive extension of these harms: cybercrimes against women. Often viewed as a modern form of victimization, these crimes leverage technology to inflict psychological, emotional, and sometimes physical distress, highlighting how offline gender inequalities are amplified and perpetuated in online spaces (European Parliament, n.d.). This essay will delve into the underlying causes that make women disproportionately vulnerable to digital aggression, explore the various forms these cybercrimes take, examine the pervasive statistical trends, discuss pivotal judicial responses in India, and finally, consider the profound victimological perspective of women affected by these digital harms.

### **Understanding Vulnerability: Why Women Become Targets**

The causes of cybercrime against women are deeply rooted in societal structures and patriarchal norms, mirroring the power imbalances that exist in the physical world. It's often observed that women are, unfortunately, perceived as more susceptible targets, a perception that digital platforms can exploit.

One contributing factor is the persistent societal view that women are often seen as "prey", a deeply troubling notion that translates into online spaces where anonymity can embolden perpetrators. This perception stems from entrenched gender biases and a culture that, in many instances, fails to adequately address the root causes of gender-based violence (European Parliament, n.d.). Online, this manifests as a sense of entitlement from aggressors, who may feel justified in harassing, objectifying, or controlling women without immediate physical repercussions.

Furthermore, it is often argued that women can be "easy to be trapped" through various social engineering tactics (CyberTalents, n.d.). Cybercriminals exploit human

vulnerabilities, such as trust, empathy, or the desire for connection. Women, perhaps more frequently exposed to social engineering scams or online grooming tactics, might be more susceptible to deceptive schemes that ultimately lead to their exploitation or victimization (Jogulamba Gadwal Police, n.d.). This is not a reflection of inherent weakness, but rather a consequence of sophisticated manipulation techniques employed by perpetrators.

Economic disparities also play a significant role; when women are economically weak, they might be more vulnerable to financial scams, phishing attempts, or blackmail (GeeksforGeeks, n.d.). The promise of quick money or a better life can be a powerful lure, exploited by criminals to gain access to personal information or financial resources, leading to severe economic and emotional distress. This economic vulnerability can also limit their access to resources needed for digital literacy, protection, or legal redress.

Perhaps one of the most heartbreaking realities is that women are more often victimized by a known person rather than an unknown individual (GeeksforGeeks, n.d.). This highlights the insidious nature of intimate partner violence (IPV) and crimes committed by acquaintances, where pre-existing trust and access to personal information are leveraged for digital abuse. Former partners, disgruntled friends, or even family members can exploit intimate knowledge to harass, defame, or blackmail, making the betrayal even more profound and difficult to address. The emotional toll of such betrayal often far outweighs the technical aspects of the crime.

### **Types of Cybercrimes Against Women**

Cybercrimes against women manifest in a multitude of ways, ranging from insidious harassment to severe violations of privacy and dignity. These acts often share commonalities with offline crimes but are amplified by the internet's reach and the perceived anonymity it offers.

One of the most prevalent forms involves sending offensive messages and emails, flooding mailboxes with unwanted content, or disseminating objectionable material, including pornography (Startertutorials, n.d.). This can range from sexually explicit images or videos to hate speech and threats, designed to intimidate, humiliate, or silence the victim. For children, particularly young girls, child pornography and obscenity represent an abhorrent crime, involving the circulation of sexually abusive material. Reports, such as those from the National Crime Records Bureau (NCRB) in India, consistently indicate that girl children are disproportionately victimized in such cases, suffering irreversible psychological trauma (The Red Team Labs, n.d.).

Beyond child victims, young women also face significant threats, particularly through intrusion of privacy and extortion. This often involves perpetrators secretly capturing or deceiving women into sharing intimate pictures or videos of their private lives, which are then used for blackmail (GeeksforGeeks, n.d.). The fear of reputational damage, family shame, or social ostracization makes this a particularly potent weapon for criminals. A significant concern in many countries, including India, is the prevalence of online chatting and cyber grooming, where adults manipulate and build relationships with minors or vulnerable individuals online with the intention of exploitation (Startertutorials, n.d.).

Cyberstalking is another deeply unsettling crime, where a perpetrator persistently follows and monitors a woman online against her wishes, using electronic media, emails, or other digital platforms (Startertutorials, n.d.; GeeksforGeeks, n.d.). This relentless digital pursuit can create immense fear and anxiety, making the victim feel constantly watched and unsafe even in their own home.

Other notable forms of cybercrime targeting women include:

- **Cyber Defamation:** Spreading false, malicious, or damaging information about a woman online, often through social media or websites, to harm her reputation (Startertutorials, n.d.).
- **Sexual Harassment on Social Media:** Unwanted sexual advances, inappropriate comments, sending unsolicited explicit content, or other forms of sexually charged communication through social media platforms.
- **Identity Theft:** Stealing a woman's personal identifying information, such as her name, address, financial details, or social security number, to commit fraud or other crimes in her name (CyberTalents, n.d.; GeeksforGeeks, n.d.).
- **Voyeurism:** Secretly observing, recording, or broadcasting a woman in private moments without her consent, often for sexual gratification (often covered under laws related to privacy violation).
- **Morphing:** The digital alteration of a woman's image, typically by superimposing her face onto explicit or compromising content, to defame, humiliate, or blackmail her. This often results in "deepfake" pornography which can have devastating consequences.

These various forms of cybercrime collectively underscore the urgent need for robust protective measures and a heightened societal awareness to safeguard women in the digital realm.

### Statistical Insights into Cybercrime Against Women

The alarming rate at which cybercrime against women is escalating is evident in recent statistics. According to the National Crime Records Bureau (NCRB) report for 2016, there were 12,317 reported victims of cybercrime, a significant increase from 11,592 in 2015 and 9,622 in 2014 (NCRB, 2016). This upward trend underscores the growing prevalence and impact of digital offenses.

A closer look at the types of cybercrimes affecting women reveals specific patterns of victimization. Out of the total chargesheeted cybercrimes in 2016 (3,712 cases), a substantial number targeted women's dignity and safety. Insulting the modesty of women accounted for 669 cases, while extortion or blackmailing of women stood at 570 cases. Sexual exploitation was reported in 562 instances, and damaging the reputation of a woman online comprised 447 cases (NCRB, 2016). These figures highlight that emotional and reputational harm, often intertwined with sexual exploitation and financial extortion, are dominant forms of cybercrime against women. Geographically, Uttar Pradesh recorded the highest number of cybercrimes against

women, with Maharashtra following as the second highest, indicating regional hotspots for these digital offenses (NCRB, 2016).

### Legal Frameworks and Protections

Addressing cybercrimes against women requires a multi-faceted legal approach, encompassing constitutional safeguards, national legislation, and international conventions. While no single law can perfectly cover the complexities of digital offenses, various provisions aim to provide protection and facilitate justice.

In India, several legal provisions form the backbone of protection against cybercrimes, drawing from both constitutional principles and specific statutes. The Indian Constitution provides fundamental rights that extend to the digital sphere. Article 21, the right to life and personal liberty, is broad enough to encompass a woman's right to dignity, privacy, and safety in online environments. Any act that infringes upon her personal space, reputation, or mental well-being online can be seen as a violation of this fundamental right. This interpretation was reinforced by the landmark *K.S. Puttaswamy v. Union of India (2017)* judgment, which recognized the right to privacy as a fundamental right under Article 21, thereby strengthening legal grounds against digital intrusions and data exploitation. Furthermore, Article 15(3) empowers the state to make special provisions for women and children, allowing for specific laws and policies aimed at protecting them, including from digital harms. The Supreme Court's ruling in *Consumer Education and Research Centre v. Union of India (1995)*, which affirmed health and medical care as a fundamental right under Article 21, further illustrates the expansive interpretation of this crucial constitutional provision, laying a precedent for protecting well-being, even in the context of digital threats.

The Indian Penal Code (IPC), though traditionally focused on physical crimes, has sections that can be applied to cybercrimes, particularly after relevant amendments. The Criminal Law (Amendment) Act of 2013, enacted in response to the heinous Nirbhaya incident, significantly bolstered protections for women by incorporating new sections from 354A to 354D into the IPC.

- **Section 509:** Addresses words, gestures, or acts intended to insult the modesty of a woman, which can include offensive messages or digital displays.
- **Section 354A (Sexual Harassment):** Covers unwelcome physical contact, demands or requests for sexual favors, and showing pornography against the will of a woman. This can certainly extend to online acts.
- **Section 354B (Assault or use of criminal force to disrobe a woman):** While seemingly physical, the threat or dissemination of material aimed at disrobing or humiliating can fall under its purview if linked to an online act.
- **Section 354C (Voyeurism):** Specifically criminalizes capturing or disseminating the image of a woman engaging in a private act without her consent. This is highly relevant to "revenge porn" and secret filming.

- **Section 354D (Stalking):** Defines and criminalizes following a person and contacting them repeatedly against their will, explicitly including communication through "any electronic communication" or monitoring their "use of the internet, email or any other electronic communication." This directly addresses cyberstalking.

Beyond the IPC, the Domestic Violence Act 2005 can also provide a framework where digital harassment is part of a pattern of domestic abuse. The Indecent Representation of Women (Prohibition) Act 1986 also holds relevance in the digital age, prohibiting the indecent representation of women in publications, which can be extended to digital content. Critically, the Information Technology Act, 2000 (IT Act), as amended, is specifically designed to address cybercrimes, acting as the primary special law in this domain. While the original IT Act lacked specific provisions for many cybercrimes, the IT Act Amendment of 2008 introduced crucial sections aimed at addressing women-related offenses. Notably, Section 66A, dealing with sending offensive messages through communication services, was inserted, alongside Sections 66C (identity theft), 66E (violation of privacy), 67A (publishing or transmitting sexually explicit material), and 72 (breach of confidentiality and privacy) (GeeksforGeeks, n.d.). The enactment of the IT Act 2000 also led to the insertion of Section 29A into the IPC, which states that "document" includes an electronic record. This crucial amendment ensures that crimes committed through electronic media can be recognized and prosecuted under the IPC, bridging the gap between traditional law and the digital realm.

Internationally, several conventions aim to address women's rights and cybercrime. The Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), a landmark treaty, obliges states to eliminate discrimination against women in all its forms. This broadly extends to violence and harassment faced by women in digital spaces. The International Covenant on Civil and Political Rights (ICCPR) provides for the protection of privacy and dignity, fundamental rights that are often violated in cybercrimes against women. While the International Covenant on Economic, Social and Cultural Rights (ICESCR) is less direct, it emphasizes women's rights in society, which are undermined by digital harms.

Perhaps the most direct international legal instrument is the Budapest Convention on Cybercrime, adopted by the Council of Europe in 2001. This treaty is significant as the first international convention on cybercrime, aiming to harmonize national laws, improve investigative techniques, and increase cooperation among states. While India is not a signatory, the convention serves as a global benchmark and influences national cybercrime legislation worldwide, promoting a unified approach to combating digital offenses.

### Judicial Responses in Indian Cyber Law

The Indian judiciary has played a crucial role in interpreting and applying existing laws to cybercrimes, even in the absence of highly specific legislation. Early cases highlighted the need for legal evolution.

One of the earliest and most notable cases of cyberstalking in India was Ritu Kohli's case. Ritu Kohli filed a complaint alleging online impersonation, the sharing of her personal information, abusive language, and the unauthorized

distribution of her mobile number, leading to unwanted calls at odd hours. This case was a landmark as the first reported cyberstalking incident against a woman in India. Initially, without a specific section under the IT Act, 2000, the case was registered under Section 509 of the IPC, which pertains to outraging the modesty of a woman. However, the legal proceedings highlighted a critical technical challenge: Section 509 of the IPC, in its original form, primarily addressed physical acts, creating a lacuna for purely cyber acts (Ritu Kohli Case, n.d.). This very challenge underscored the pressing need for specific cybercrime legislation, leading to the pivotal amendment of the IT Act, 2000, and the insertion of Section 66A in 2008 to specifically address offensive messages sent via communication services (Ritu Kohli Case, n.d.).

While Section 66A was a significant step, its broad wording eventually led to controversy. The Supreme Court in the landmark case of *Shreya Singhal v. Union of India* (2015), famously struck down Section 66A of the IT Act, 2000, deeming it unconstitutional. The court ruled that the section violated the fundamental right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution, citing its vagueness and chilling effect on free speech. This judgment, while protecting civil liberties, also necessitated a re-evaluation of how online offenses, particularly those targeting women, would be addressed.

Other significant cases that have shaped the judicial landscape include:

- **Avinash Bajaj v. State (2008)** <sup>[1]</sup>: This case involved the uploading of obscene MMS clips, leading to charges under the IT Act and IPC. It was an early instance of a high-profile case dealing with digital content.
- **State of Tamil Nadu v. Suhas Katti (2004)** <sup>[18]</sup>: Considered one of India's first cybercrime convictions, this case involved a man posting defamatory content about a divorced woman on an online message board. The accused was convicted under Section 67 of the IT Act, 2000, for publishing obscene material.
- **Sushil Ansal v. State through NCT of Delhi (2014)** <sup>[19]</sup>: While primarily related to the Uphaar Cinema tragedy, this case also involved aspects of media reporting and potential contempt of court, highlighting the judiciary's engagement with various forms of information dissemination, including digital.

These judgments, collectively, reflect the Indian judiciary's ongoing efforts to adapt traditional legal principles to the rapidly evolving digital environment, balancing the need for protection with constitutional freedoms.

### Victimological Perspective of Cybercrime on Women

The true impact of cybercrime against women extends far beyond legal definitions and statistics; it delves into the profound psychological, emotional, and social consequences suffered by victims. The NCRB report from 2016 noted 12,317 victimized individuals, each with a unique story of distress and disruption (NCRB, 2016). Women suffer immensely from cybercrimes, often leading to a cascade of negative effects that can be deeply isolating and long-lasting.

**Psychological Impact:** Women who experience cybercrimes often grapple with intense feelings of insecurity and profound mental disturbance. The constant threat of digital harassment, the violation of privacy (especially through non-consensual image sharing), or the fear of intimate images being leaked can lead to severe anxiety, depression, and even post-traumatic stress disorder (PTSD). The digital nature of the crime means that the perpetrator can feel omnipresent, eroding the victim's sense of safety even in their own home. Unlike physical crimes, cybercrimes often leave no visible scars, making it harder for others to grasp the severity of the trauma, which can lead to feelings of isolation and invalidation for the victim. These attacks can deeply affect a woman's self-esteem, leading to persistent feelings of shame, embarrassment, and self-blame.

**Physical Impact (Indirect):** While cybercrimes are not physical in nature, their psychological toll can manifest in physical symptoms. Victims may experience sleep disturbances, chronic stress, eating disorders, and a general decline in physical health due to the immense mental strain. In extreme cases, the pressure and despair can tragically lead to self-harm or suicidal ideation, highlighting the critical link between psychological distress and physical well-being. The constant state of alarm can also compromise the immune system, making victims more susceptible to illnesses.

**Financial Loss:** Many women are significantly affected financially due to online frauds, scams, and extortion. The loss of money through phishing attacks, deceptive investment schemes, or blackmail can be devastating, impacting their economic independence and future stability. In some heartbreaking instances, women are deceived in the name of marriage or love, falling prey to online romantic scams that exploit their emotional vulnerabilities for financial gain or other forms of exploitation. The emotional investment in such relationships makes the eventual betrayal all the more crushing, compounding the financial devastation.

**Family Disturbance:** The ripple effect of cybercrime often extends to the victim's family. The revelation of online harassment, particularly involving intimate content or defamation, can lead to immense family disturbance. Families may struggle with feelings of shame, anger, confusion, and helplessness. This can strain relationships, leading to conflict or, tragically, the victim being blamed or ostracized by her own loved ones due to societal stigma. The family's privacy might also be compromised if the cybercriminal targets them directly or indirectly.

**Isolation:** A particularly challenging aspect of cybercrime against women is the profound social stigma associated with it, which often leads to isolation. Many victims find themselves unable to discuss the incident, even with their closest family members or friends. This silence is often fueled by fear of judgment, shame, or the societal tendency to blame the victim for "allowing" the crime to happen. The reputation of the woman, and by extension, her family, can feel irrevocably damaged, trapping victims in a cycle of silence and suffering. This lack of disclosure hinders reporting, support, and ultimately, justice, pushing victims

further into isolation and making recovery even more difficult. The inherent characteristics of technology-based crimes—their speed to reach audiences, ease of access for perpetrators, and the rapid, widespread reaction they can elicit—contribute to an increased rate of victimization, amplifying the sense of helplessness and isolation as malicious content spreads virally.

In essence, cybercrimes against women are not merely digital offenses; they are deeply personal attacks that shatter trust, erode self-worth, and impose a heavy, often invisible, burden. Understanding this victimological perspective is crucial for developing compassionate support systems and effective preventative strategies that acknowledge the unique challenges faced by women in the digital age.

## Conclusion

Cybercrimes against women represent a grave challenge in our increasingly interconnected world, reflecting and amplifying existing societal gender inequalities. From the insidious forms of digital harassment, such as cyberstalking and defamation, to the deeply damaging acts of voyeurism, morphing, and the dissemination of non-consensual intimate imagery, these crimes inflict profound psychological, emotional, and reputational harm on victims. The vulnerabilities that lead to women being targeted are complex, stemming from societal perceptions, economic disparities, and the alarming reality that known individuals often exploit trust to perpetrate these abuses. The statistical trends underscore the growing scale of this problem, with specific offenses like insulting modesty and extortion dominating the landscape.

While the digital landscape presents new avenues for crime, legal frameworks are continuously evolving to meet these challenges. In India, a combination of constitutional rights (particularly Article 21's expansive interpretation, reinforced by the Puttaswamy judgment), specific IPC sections (especially those bolstered by the 2013 amendment), and the crucial Information Technology Act provides a basis for legal action. Landmark judicial responses, like the Ritu Kohli case and the Shreya Singhal judgment, have shaped the application and evolution of cyber laws, highlighting both progress and ongoing challenges. Internationally, conventions like CEDAW and the Budapest Convention highlight a global commitment to addressing cybercrime and protecting women's digital safety. However, legal provisions alone are insufficient. A comprehensive approach requires enhanced digital literacy and awareness campaigns, robust reporting mechanisms, efficient law enforcement, and a societal shift towards recognizing and actively combating online gender-based violence. Only through collective effort—by individuals, communities, governments, and international bodies—can we create a safer and more equitable digital environment for women, ensuring that the promise of technology does not come at the cost of their dignity and well-being.

## References

1. Avinash Bajaj v. State, 152 DLT 73 (India), 2008.
2. Consumer Education and Research Centre v. Union of India, AIR 1995 SC 636 (India).
3. CyberTalents. What is Cyber Crime? Types, Examples, and Prevention [Internet]. [cited 2025 Jul 30]. Available from: <https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention>

4. European Parliament. Understanding cybercrime [Internet]. [cited 2025 Jul 30]. Available from: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS\\_BRI\(2024\)760356\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf)
5. GeeksforGeeks. Cyber Crime [Internet]. [cited 2025 Jul 30]. Available from: <https://www.geeksforgeeks.org/ethical-hacking/cyber-crime/>
6. Jahankhani H, Al-Nemrat A, Amin I. Definition and typologies of cybercrime [Internet]. Rudolf Agricola School, 2014 [cited 2025 Jul 30]. Available from: <https://www.rug.nl/rudolf-agricola-school/research/development-security-and-justice/cybercrime-illicit-trade.pdf>
7. Jogulamba Gadwal Police. Types of Cyber Crimes [Internet]. [cited 2025 Jul 30]. Available from: <https://www.jogulambagadwalpolice.telangana.gov.in/PDF/TYPES-OF-CYBER-CRIMES.pdf>
8. Jogulamba Gadwal Police. Types of Cyber Crimes [Internet]. [cited 2025 Jul 30]. Available from: <https://www.jogulambagadwalpolice.telangana.gov.in/PDF/TYPES-OF-CYBER-CRIMES.pdf>
9. K.S. Puttaswamy v. Union of India, 10 SCC 1 (India), 2017.
10. National Crime Records Bureau. Crime in India 2016 Statistics. Ministry of Home Affairs, Government of India, 2016.
11. Rahaman S. Cybercrime definition [Internet]. ResearchGate, 2016 [cited 2025 Jul 30]. Available from: [https://www.researchgate.net/publication/265350281\\_Cybercrime\\_definition](https://www.researchgate.net/publication/265350281_Cybercrime_definition)
12. ResearchGate. Cybercrime: History of formation, current state and ways of counteraction [Internet]. [cited 2025 Jul 30]. Available from: [https://www.researchgate.net/publication/368023408\\_Cybercrime\\_History\\_of\\_formation\\_current\\_state\\_and\\_ways\\_of\\_counteraction](https://www.researchgate.net/publication/368023408_Cybercrime_History_of_formation_current_state_and_ways_of_counteraction)
13. ResearchGate. The History of Cybercrime (1976-2016) [Internet]. [cited 2025 Jul 30]. Available from: [https://www.researchgate.net/publication/313662110\\_The\\_History\\_of\\_Cybercrime\\_1976-2016](https://www.researchgate.net/publication/313662110_The_History_of_Cybercrime_1976-2016)
14. Ritu Kohli Case. The First Cyber Stalking Case in India [Internet]. [cited 2025 Jul 30]. (Note: Specific source not provided).
15. Shreya Singhal v. Union of India, AIR 2015 SC 1523 (India).
16. SlideShare. Cyber Criminals, Classifications of Cybercrimes [Internet]. [cited 2025 Jul 30]. Available from: <https://www.slideshare.net/slideshow/cyber-criminalsclassifications-of-cybercrimes-aatpplx/253092776>
17. Startertutorials. Types of Cybercrime [Internet]. [cited 2025 Jul 30]. Available from: <https://www.startertutorials.com/blog/types-of-cybercrime.html>
18. State of Tamil Nadu v. Suhas Katti, 2004 SCC OnLine Mad 33 (India).
19. Sushil Ansal v. State through NCT of Delhi, (2014) 6 SCC 173 (India).
20. The Red Team Labs. A brief history of cybercrime [Internet]. [cited 2025 Jul 30]. Available from: [https://theredteamlabs.com/a-brief-history-of-cybercrime/#elemmonter-toc\\_heading-anchor-2](https://theredteamlabs.com/a-brief-history-of-cybercrime/#elemmonter-toc_heading-anchor-2)