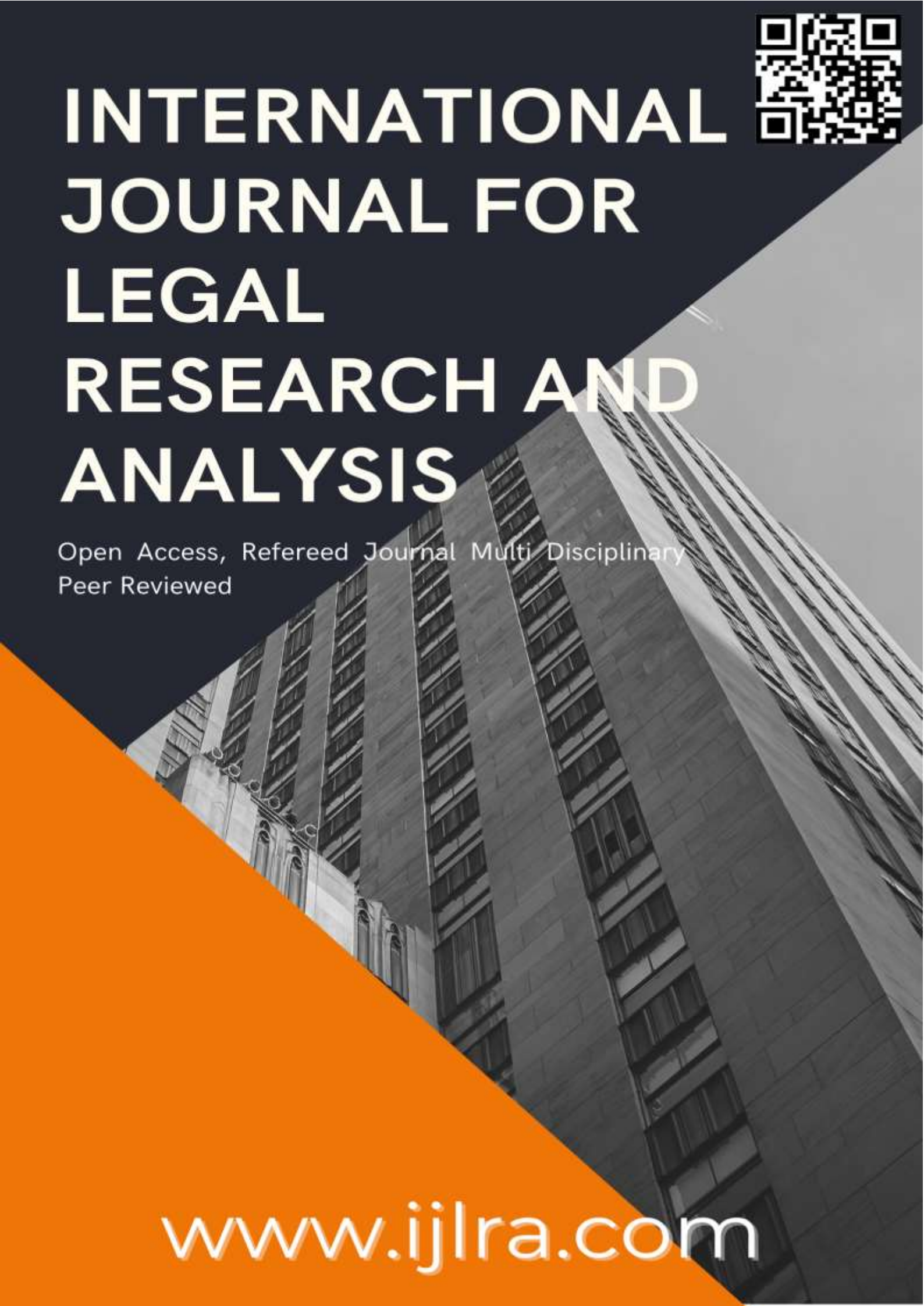
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

FROM VICTIM TO VANGUARD: LEGAL AND POLICY STRATEGIES FOR CONTAINING CYBERCRIME IN THE DIGITAL AGE

AUTHORED BY - YATHARTH UPALKAR & RACHIT TIWARI
Faculty of law, Gujarat Law Society

Abstract

Honestly, we didn't expect this topic to go so deep. Cybercrime in India isn't just some faraway thing about hackers. It's affecting people, especially women and teenagers, every day—whether it's online blackmail, stalking, or just emotional manipulation. We have come across stories where victims are left feeling helpless, even scared to use the internet again. That stuck with me.

This paper primarily aims to illustrate what they experienced. For instance, we often discuss laws—the IT Act, 2000,[1] and now the new DPDP Act from 2023[2]—but in reality, it still feels like the system isn't ready for what people are facing online. Sure, there are legal tools, and police are trying, but things like cross-border crime, lack of training, or even just victims not knowing where to go—it all adds up.

We have looked at how mental health ties into it, too. A lot of these people aren't just victims of a crime, they're dealing with anxiety, stress and sometimes depression. And many don't speak up. I think what this paper is arguing is that we need a more human approach—like, real help for real people. Because right now, we're not quite there.

Keywords-Cybercrime, Victimisation, Digital Law, Information Technology Act, Data Protection.

[1] Information Technology Act, No. 21 of 2000, § 43A, INDIA CODE
[2] Digital Personal Data Protection Act, No. 22 of 2023, § 2(7), INDIA CODE.

ISSN: 2582-6433

Introduction

The advancement of technology has brought about significant societal changes, revolutionising the way people communicate, conduct business and access information. However, this digital transformation has also given rise to new forms of criminal activity, commonly known as cybercrime[3]. Categories of cybercrime, as per the victim perspective, are divided into Violent and Non-Violent Crimes:

1. Violent Cyber Crime

A. Cyber Terrorism

Cyber terrorism is the link between cyberspace and terrorism. These are coordinated efforts by foreign intelligence agencies, cyber terrorists, or other groups to identify potential security flaws in important systems. A cyber terrorist is someone who intimidates or coerces a government or organisation to promote his or her political or social goals by conducting a computer-based attack against computers, networks, or the information stored on them[4].

B. Cyber stalking.

Cyber stalking is a sort of cybercrime in which an assailant harasses a victim through electronic means. In other cases, cyberstalking begins as physical stalking and then spreads to the internet. Cyberstalking can potentially cause personal injury in person. Harassment, shame, humiliation, threats, defamation, and other forms of abuse exacerbate the situation. Cyber stalkers are primarily driven by hatred, vengeance, jealousy, obsession, and mental instability. Cases against this offence are lodged under section 79 of the Bharatiya Nyaya Sanhita, 2023[5].

C. Pornography.

It is the first successful e-commerce product. It is easily accessed on computers, mobiles, and other smart devices. Currently, this is the most vicious category of cybercrime in which teens and adults are easily involved. Punishments for these acts are under section 67 of the Information Technology Act of 2000[6], Indecent

[3] *Makam Ganesh Kumar, Cybercrime and Electronic Evidence in India: A Comprehensive Analysis (LL.B. (Hons.) dissertation, O.P. Jindal Global Univ. 2021)*
[4] **Cybercrime**, *Wikipedia*, https://en.wikipedia.org/wiki/Cybercrime (last visited August 6, 2025)
[5] *Bharatiya Nyaya Sanhita, No. 45 of 2023, § 79 (India).*
[6] *Information Technology Act, No. 21 of 2000, § 67 (India)*

ISSN: 2582-6433

Representation of Women Prohibition Act, 1986[7] and sections 294[8], 295[9], 297[10] of BNS, 2023[11].

D. Cyberbullying.

Cyberbullying is the brief and simple stance is act of using smartphone services to frighten, threaten, or bully a person using instant messaging, email, chat rooms, or social networking Web sites. Cyberbullying victims are typically children, and it is frequently perpetrated by children who have increased access to new modern technologies. They often use fictitious names and genders to conceal their genuine identities. This anonymity helps bullies to do more than they would otherwise do since they cannot be easily traced.

2. Non-violent cybercrimes.

A. Cyber theft mostly includes

1. Cyber embezzlement - It means misuse or alteration of data by an employee of a company who has legitimate access to the company's computerised system and network
2. Unlawful Appropriation- In a case where the person acquires external access to the organisation in order to move funds & alteration of documents in a way that allows him a property right, he is not entitled to.
3. Corporate espionage- In this case, the network is used by someone already in/out of the business to access marketing strategies, rates, trade secrets, financial information, client list etc to acquire a competitive edge. In industrial or corporate espionage, an individual gets access to the company network and takes trade secrets, financial information, proprietary client contacts lists or marketing plans or any other information to provide them with competitive advantage.

B. Cyber fraud: Cyber fraud is a broad phrase used to represent crimes conducted by cyber attackers over the internet. These crimes are performed to illegally obtain and exploit sensitive information about an individual or business for financial advantage.

C. Cyber Trespass: The act of Cyber Trespass can be defined as unauthorised access to a computer or network. It entails getting unauthorised access to a system, which may or

[7] *V. Vishwanath Paranjape, Legal Dimensions of Cybercrimes and Preventive Laws 7 (1st ed. Central Law Agency 2010).*
[8] *Bharatiya Nyaya Sanhita, No. 45 of 2023, § 294 (India)*
[9] *Bharatiya Nyaya Sanhita, No. 45 of 2023, § 295 (India)*
[10] *Bha Bharatiya Nyaya Sanhita, No. 45 of 2023, § 297 (India)*
[11] *Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE*

ISSN: 2582-6433

may not include destroying, changing, or misusing data or systems

D. Destructive Cyber Crime that is Cyber Vandalism, Viruses: Destructive cybercrime is defined as harmful operations carried out via computers or networks to damage, disrupt, or destroy data, systems, or digital infrastructure.

Cyber Vandalism is the deliberate defacement, alteration, or destruction of digital content, such as hacking into websites to modify their appearance, destroy data, or distribute inappropriate material. It is comparable to real vandalism, but occurs in the virtual world, and is frequently intended to cause shame, reputational injury, or operational inconvenience.

Viruses are malicious software programs that penetrate a computer system without the user's knowledge, duplicate themselves, corrupt files, or disrupt operations. Viruses can erase data, slow down computers, or render them unworkable, and they are frequently propagated via infected files, email attachments, or malicious downloads.

E. Other non-violent Cyber Crimes that are Cyber Prostitution, Online Gambling, Cyber Laundering, and Internet Drug Sales:

Cyber prostitution is the use of the internet, social media, or online platforms to advertise or organise sexual services in return for money or other benefits. It frequently includes anonymity, encrypted communication, and internet advertising, making it difficult for law enforcement to track.

Online gambling is defined as the participation in or operation of betting, casino, or lottery activities via websites and mobile applications without a legal license. Such platforms may circumvent national laws, exploit regulatory gaps, and lead to financial crime or addiction.

Cyber Laundering is the process of leveraging internet technologies, digital currencies, or electronic transactions to conceal the origin of illegally obtained funds. Criminals use many digital accounts, gaming platforms, or cryptocurrency wallets to make their transactions appear real.

Internet drug sales refer to the sale, advertising, or distribution of illegal or controlled narcotics via websites, encrypted messaging applications, or dark web markets. To avoid detection, transactions are sometimes camouflaged utilising bitcoin and disguised shipping methods.

Furthermore, Cybercrime is classified into three subtypes[12]:

[12]*The International Journal of Indian Psychology, ISSN 2348-5396 (electronic), ISSN 2349-3429 (print)*

ISSN: 2582-6433

1. Cyber-Dependent
2. Cyber-Enabled
3. Cyber-Assisted

Legal Framework for Cybercrime in India

Addressing cybercrime in India requires a robust legal framework that defines offences, prescribes penalties, and establishes mechanisms for investigation, prosecution, and prevention. The key legislation governing cybercrime in India is the Information Technology Act, 2000 (IT Act)[13].

1) The Information Technology Act, 2000[14]

The Information Technology Act, 2000[15], acts as the cornerstone of cybercrime legislation in India. It provides a comprehensive framework to address various cyber offences, including unauthorised access, data theft, computer-related offences, and hacking. The Act empowers law enforcement agencies to investigate cybercrimes and outlines procedures for the search and seizure of electronic evidence. It also constitutes the Cyber Appellate Tribunal to appeal against the orders of the Adjudicating Officer under the Act.

2) Key Amendments to the Information Technology Act, 2000

Recognising the evolving nature of cybercrimes, the IT Act[16] underwent several amendments to strengthen its provisions and align them with emerging challenges. The Information Technology (Amendment) Act, 2008[17], made significant amendments to handle emerging kinds of cybercrime and strengthen penalties for offences such as cyber terrorism, identity theft, and breach of confidentiality. The amendment also included regulations governing data protection, interception, and monitoring of electronic communications.

3) Other Relevant Laws and Regulations

In addition to the IT Act[18], other laws and regulations supplement the legal framework for cybercrime in India. The Bharatiya Nyaya Sanhita, 2023[19], encompasses provisions that can be

[13] *Information Technology Act, No. 21 of 2000, INDIA CODE*
[14] *ibid*
[15] *ibid*
[16] Information Technology Act, No. 21 of 2000, INDIA CODE
[17] ibid
[18] ibid
[19] Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE

ISSN: 2582-6433

applied to cybercrimes, such as fraud, defamation, or stalking. The Criminal Procedure Code, 1973[20], governs the investigation and prosecution of cybercrime cases. The Reserve Bank of India Act, 1934[21], and the Payment and Settlement Systems Act, 2007[22], provide regulatory measures related to financial cybercrimes and the digital payment system.

Electronic Evidence & the Evidence Act

Furthermore, the Section 92 of the Information Technology Act[23] revised the Indian Evidence Act;[24] the definition of evidence now includes "electronic record" for making electronic evidence admissible. Section 59[25](54 BSA)[26] "documentary evidence" now "contents of documents or electronic records" instead of "contents of documents". Furthermore, sections 65A[27](62 BSA)[28] and 65B[29](63 BSA)[30] were amended to allow electronic evidence admissibility. Section 79A of the IT Act[31] broadened Section 45[32](39 BSA)[33] of the Indian Evidence Act. Section 45[34](39 BSA)[35] of the IEA covers expert opinion. Section 45[36](39 BSA)[37] of the IEA states, "When there is a requirement as to the formation of opinion by the Court of law on the points such as foreign law or of science or art or identification of handwriting or finger impressions, the opinions of such persons shall be relevant on that point who are especially skilled in that field." This section considers expert viewpoints. In 2009, Section 45A[38] was added to make the "*Opinion of the Examiner of Electronic Evidence applicable in court*". Section 45A[39](39 BSA)[40] states that "*an Examiner of Electronic Evidence under Section 79A[41] of the Information Technology Act, 2000 is a relevant fact if the Court*

[20] Code of Criminal Procedure, No. 2 of 1974, INDIA CODE
[21] Reserve Bank of India Act, No. 2 of 1934, INDIA CODE
[22] Payment and Settlement Systems Act 2007 (India)
[23] Information Technology Act, No. 21 of 2000, § 92 (India)
[24] Indian Evidence Act, No. 1 of 1872 (India)
[25] Indian Evidence Act, No. 1 of 1872, § 59A (India)
[26] Bharatiya Sakshya Adhiniyam 2023, No. 46 of 2023, § 54 (India)
[27] Indian Evidence Act, No. 1 of 1872, § 65A (India)
[28] Bharatiya Sakshya Adhiniyam, No. 46 of 2023, § 62 (India)
[29] Indian Evidence Act, No. 1 of 1872, § 65B (India)
[30] Bharatiya Sakshya Adhiniyam, No. 46 of 2023, § 63 (India)
[31] *Information Technology Act, No. 21 of 2000, § 79A (India)*
[32] *Indian Evidence Act, No. 1 of 1872, § 45 (India)*
[33] *Bharatiya Sakshya Adhiniyam, No. 46 of 2023, § 39 (India)*
[34] *Ibid 32*
[35] *Ibid 33*
[36] *Ibid 32*
[37] *Ibid 33*
[38] *Indian Evidence Act, No. 1 of 1872, § 45A (India)*
[39] *ibid*
[40] *Ibid 33*
[41] *Ibid 31*

ISSN: 2582-6433

needs to form an opinion on any matter involving information communicated or stored in any computer resource or other electronic or digital form". The addition of the clause to the explanation section 45A[42], indicates that the Examiner of Electronic Evidence is an expert in this section.

Furthermore, Section 65A[43] of the Indian Evidence Act provides for electronic records in accordance with Section 65B[44]. Thus, Section 65B[45] of the Evidence Act describes how to justify electronic documentary evidence. Despite the other provisions of the Evidence Act, any information that was in an electronic record-engraved on a paper, stored, recorded, or copied in optical or magnetic media that was generated by a computer-will qualify as a document provided that it satisfies the conditions set out under section 65B (2) to (5)[46] in connection with the information and the computer. Electronic evidence admissibility should be based on Section 65B (2) to (5)[47]. The Hon'ble Supreme Court in the case of Anvar P.V. Vs. P.K. Basheer and Others[48] critically examined that computer output must comply with Section 65B[49]. The Hon'ble Supreme Court division bench ruling in the case of State (NCT of Delhi) versus Navjot Sandhu[50] was overturned as "*The Judgement of Navjot Sandhu, to the extent, the statement of the law on admissibility of electronic evidence pertaining to electronic record of this court, does not lay down correct position and is required to be overruled,*". Furthermore, the Apex Court addressed criminal evidence admissible in Tomaso Bruno & Anr. Vs. State of UP[51]. The Hon'ble Court ruled that "*the computer-generated electronic records in evidence are admissible at a trial if proved in the manner specified by Section 65B[52] of the Evidence Act*". Paper prints of electronic records stored in an optical or magnetic medium created by a computer are accepted as documents under sub-section (1) of Section 65B[53], provided the conditions in sub-section (2)[54] are met. And thus, the Section 65[55] of the Evidence Act allows secondary document content evidence.

[42] *Ibid 38*
[43] *Indian Evidence Act, No. 1 of 1872, § 65A (India)*
[44] *Indian Evidence Act, No. 1 of 1872, § 65B (India)*
[45] *ibid*
[46] *Indian Evidence Act, No. 1 of 1872, §§ 65B(2)–(5) (India)*
[47] *ibid*
[48] *Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India)*
[49] *Ibid 44*
[50] *State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 S.C.C. 600 (India)*
[51] *Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 S.C.C. 178 (India)*
[52] *Indian Evidence Act, No. 1 of 1872, § 65B (India)*
[53] *Indian Evidence Act, No. 1 of 1872, § 65B (1) (India)*
[54] *Indian Evidence Act, No. 1 of 1872, § 65B (2) (India)*
[55] *Indian Evidence Act, No. 1 of 1872, § 65 (India)*

ISSN: 2582-6433

Jurisdictional Challenges in Prosecuting Cybercriminals

Cybercrimes can easily cross geographical borders giving it jurisdictional issues to law enforcement agencies. The cyberspace makes it hard to establish jurisdiction because the internet is global and technology offers anonymity. International collaboration and mutual legal assistance will play a pivotal role in the process of investigating and prosecuting cybercriminals who work in other countries. However, there are general international law principles that are applicable, e.g. the principle of territoriality.

Victim Perspective-Cyber Crime

"*It is said that technology is an overpowering power; it has taken away the Green browsers. It was introduced for a good use, but now has only become a misuse.*"[56]

The following adage is correct, as technology in the present period has become a curse for people. Cybercrime is a computer-related crime. This is a computer and network-related crime. These cover a wide range of illegal actions. Cybercrime is a broad phrase that encompasses a wide range of criminal behaviours. The form of crime defined above as cybercrime is an offence that is committed against a person or a group of persons with a criminal intent to defame the person or persons directly or indirectly with the use of modern telecommunication networks like the internet and cell phones. Cybercrime criminals can endanger an individual or state, safety and financial wellness. Today, such kinds of crime have become high profile especially those that are involved in hacking, copyright infringement, unreasonable mass surveillance, sex trafficking, child pornography, child grooming, Digital rights and individual rights infringement.

With that, the primary concern today is cybercrime against women, which occurs when a crime is committed against a woman to intentionally injure or denigrate the victim psychologically or physically, using contemporary telecommunication networks such as the internet or mobile phones. This form of crime against women is increasing daily, and at a rapid pace. Women are targeted on the internet, their personal information is demanded, and they are ultimately blackmailed by those persons. People are often given job offers, and when they take them, they get trapped, which leads to crime against them. It has been reported that women go missing

[56] *Vishi Aggarwal & Shruti, Cybercrime Victims: A Comprehensive Study, 6* ***Int'l J. Creative Res. Thoughts*** *2 (Apr. 2018), https://ijcrt.org/papers/IJCRT1807078.pdf (last visited August 6, 2025)*

ISSN: 2582-6433

after seeing their social media connections.[57]

There are risk factors for this criminal activity. There are four major factors: **history of antisocial behaviour, antisocial personality pattern, antisocial cognition, and antisocial associates**. This is followed by four moderate factors namely family/marital status, school/work, leisure/recreation, and substance misuse. The victims of person-centred cybercrime, those whose acquaintances or perpetrators are less likely to experience long-term financial and logical consequences, mental illness, and psychological tensions can become victims of personality-based cybercrime, and anxiety levels rise in the victims of identity theft or online privacy offences.

Victims of person-centred cybercrime, those who, whose acquaintance or the offenders, and those who do not receive financial loss, compensation, and more likely to experience a long-term, financial and cycle logical report, questions, mental illness, psychological tensions, may make a victim of cybercrime, more susceptible to it with that anxiety may increase in those who become victims of identity theft or online privacy violation.

It might be upsetting to worry about money, regulations, reputational damage, or the misuse of personal information. The consequences of cybercrime, including but not limited to identity theft, cyberbullying, online harassment, and financial loss, can have a significant impact on a person's psychological state, dismissal, and despairing actions, which can lead to suicidal thoughts, despair, helplessness, and hopelessness. Increased anxiety, fury, despair, and post-traumatic stress disorder symptoms, such as vivid flashbacks of traumatic events, can lead to intrusive thoughts and acute suffering when exposed to symbolic reminders of the trauma.

The effects of cybercrime, among others, cyberbullying, identity theft, the loss of money, and online harassment, may significantly affect the psychological state of a person evoking behaviour that may result in suicidal ideations, despair, helplessness, and hopelessness. Anxiety, anger, hopelessness, and symptoms of post-traumatic stress disorder which include vivid flashbacks about the traumatic experience can cause intrusive thoughts and acutely painful experiences upon exposure to symbolic reminders of the trauma. In order to overcome the trauma, the victims of cybercrime employ negative coping mechanisms. Such techniques

[57] *Ankur Singh, New Wave: Cybercrime Against Women,* ***OneIndia.com*** *(Oct. 11, 2024), https://www.oneindia.com/india/new-wave-cyber-crime-against-women-1894591.html (last visited July 6, 2025).*

ISSN: 2582-6433

include passive, pretty alcohol, use avoidance, worsening their mental health, and the rate of cyberstalking is more frequent among women, and younger adult victims are more prone to reach utter desperation. Due to the application of negative coping mechanisms such as reading, passivity and avoidance.

Techniques for coping, such as the consumption of alcohol and avoidance techniques, are used, which exacerbate their psychological well-being. Cyberstalking is more common in women, and younger adult victims are more likely to experience profound depression. As a result of engaging in poor coping strategies such as reading, inactivity, and avoidance.

The coping strategies for cyber victims are of two types.

1. Positive coping strategies, first emotional focused or seeking support, mindfulness, physical activities, and positive affirmations.
2. Problem, focus report, the incident, she quickly advises: change, password, educate oneself.

Negative cooking strategies of substance, abuse, avoidance, denial, venting, aggression, positivity.

Role of Law Enforcement Agencies & Digital Forensics

The policing mechanism in India is mainly of two types: firstly, the dual control system of policing[58] and secondly, the Commissionerate system of policing.

Under the dual police system, the District Superintendent of Police is in charge of the entire force, while the District Magistrate has overall authority and direction. The dual system caused numerous obstacles to the force's effective governance due to a lack of clarity in the delegation of functions between the Superintendent and Magistrate. This resulted in perpetual conflict and disorder, particularly in metropolitan cities with high population density and unique law and order problems, prompting the introduction of the Commissionerate system. Under this arrangement, a city's Commissioner of Police is in charge of policing it.

[58] *Police Act, No. 5 of 1861, § 4 (India)*

ISSN: 2582-6433

"*Cyber Security is crucial, Govt. Websites also get hacked and misused, due to which the public is often misled with information,*"-Justice Lokar[59]

The process of enactment of laws is a significant aspect of addressing a particular kind of issues in the society; however, enactment of laws without enforcement does not have any positive effect. Here the need to look into the important role played by the law enforcement agencies or in simpler terms, the national police force, emerges. The police have also been given authority to perform important roles especially in fighting cybercrime as a result of the legislation.

An example is the Information Technology Act of 2000[60], which permits police to enter any place which is open to the general public and search and arrest without warrants anyone found there who is suspected reasonably as having committed, committing, or about to commit an infraction under the Act. Moreover, all the information or matter provided or made accessible in an electronic form that can be used subsequently is considered legally as evidence, which grants the police the right to perform searches and retrieve electronic evidence. The overall process of investigating a cybercrime can be described as follows: creating a sophisticated strategy, refusing additional access to the attacked computer resource, taking measures of precaution to make sure that the investigation will proceed smoothly, involving a forensic expert in case of a specialist seizure of all items, and safeguarding and delivering the data collected safely. Cyber-policing in the country is regulated by the Central Bureau of Investigation (CBI). The main institutions that are in charge of investigations in cybercrimes include the Cyber Crime Research and Development Unit, Cyber Crime Investigation Cells, Cyber Forensic Labs, and Network Monitoring Centres. The following are some of the major bodies in charge of cybercrime detection and investigation in the country. They make sure that they cooperate with the State Police Force as well as ensuring that they investigate and pursue the actions of Inspecting Officers (IO) on critical cases.

Moreover, forensic labs have been erected in every district to facilitate the prevention and detection of cybercrime. One of the most important innovations of the Central Bureau of Investigation is the Cyber and High-Tech Crime Investigation and Training Centre (CHCIT). It functions out of the CBI Academy. The centre has also helped in technological and forensic investigations in the high-profile cases.

---

[59] *International Conference on Cyber Law, Cyber Crimes and Cyber Security 2016,* ***Int'l Conf. on Cyber Law, Cyber Crimes & Cyber Security*** *(June 23, 2018, 9:00 AM), http://cyberlawcybercrime.com/previousiccc/iccc-2016 (last visited August 6, 2025)*

[60] *Information Technology Act, No. 21 of 2000, INDIA CODE*

ISSN: 2582-6433

They also ensure collaboration with the State Police Force and are the ones to investigate and further the action of an Inspecting Officer (IO) in critical cases. Moreover, forensic laboratories are set up in every district to assist in preventing and detecting cybercrime. Central Bureau of Investigation has a significant innovation- the Cyber and High-Tech Crime Investigation and Training Centre (CHCIT). It operates at the CBI Academy. The centre has assisted with technological and forensic investigations in high-profile instances.[61]

The primary law in India that governs internet-related offences is the Information Technology (IT) Act, 2000[62], which has been enforced by the Ministry of Electronics and Information Technology, forming a cornerstone of cyber law in India. It stipulates reasonable security practices and procedures to be followed by corporations to protect sensitive personal data or information, crucial for preventing cybercrimes in India. Predominantly, law enforcement agencies employ the stipulations of this act to combat a wide array of digital crimes, which range from cyber-harassment and fraud to more sophisticated forms of criminal activities such as ransomware and identity theft. These agencies also work diligently to keep abreast of advancing technology and to intercept any issues related to digital crimes. Cybercrimes, specifically those that involve a computer as the object or subject of the crime, have seen a significant increase in the last decade. The number of cybercrimes reported under the IT Act has markedly escalated, reflecting a disturbing global trend. This indicates the crucial role o[63]f Indian laws and enforcement agencies in exploring new ways to curb this rising problem and ensure a safer digital space.

Case Studies: Instances of Online Crimes and Legal Action in India

India has witnessed an alarming increase in cybercrime cases, and the internet has become a hotbed of cyber threats, underlining the urgent need for robust cybersecurity measures and cyber law in India. This necessitated robust guidelines for intermediaries and digital media ethics to ensure a secure and healthy digital space, aligning with the principles of cyber law in India. The Ministry of Electronics and Information has been proactive in addressing this cyber risk by formulating laws, regulations, and necessary amendments to contain these instances of online offences. Intermediaries and digital entities that breach these guidelines are liable to be

[61] *Cyber & Hi-Tech Crime Investigation & Training Centre (CHCIT) Overview*, ***CBI Acad.*** *(June 26, 2018, 12:00 PM), http://www.cbiacademy.gov.in/chcit.php (last visited August 6, 2025)*
[62] *Information Technology Act, No. 21 of 2000, INDIA CODE*
[63] *ibid*

ISSN: 2582-6433

penalised according to the law. For instance, under Section 66 of the IT Act[64], a person guilty of committing cybercrime "*shall be punished with imprisonment up to three years or with a fine which may extend to up to five lakh rupees, or with both*". Similarly, according to the guidelines for intermediaries and digital services, if they fail to abide by the rules or regulations made thereunder, they may be subject to a term that may extend to seven years and also a fine. Various law enforcement agencies have been diligently working to ensure that such legal provisions under the India Act are implemented effectively to combat types of cybercrimes.

Challenges in Implementing Laws against Online Crimes

The aptitude to combat online offences is consistent with the importance of cyber law in India, including cybercrimes that can be far-reaching in scope and impact. This battle is not without its difficulties. First and foremost, the definition of cybercrime is multifaceted, encompassing a variety of activities, from unauthorised use of computer systems without the permission of the owner to the manipulation of data to alter any computer source code. With advancements in technology, new forms of infractions are emerging, often quicker than the legislation can adapt. The effective prevention of cybercrimes is further complicated by legal provisions such as the 'Reserve Bank of India Act' that lack explicit consequences for internet-based offences. While the IT Act states that tampering with a computer source code used for a particular application shall be punishable, the ambiguity surrounding the enforcement of these rules poses a significant challenge. Moreover, the inherently borderless nature of the internet exacerbates these challenges, as activities related to online crimes can originate and propagate across various jurisdictions, complicating the enforcement efforts.

Future of Digital Law: Potential Amendments and Reforms

As the digital landscape continues to evolve at an unprecedented pace, it is clear that the code used for computers and their applications will also transform rapidly. To better cope with this dynamic environment and combat cybercrime effectively, potential amendments and reforms in digital law are on the horizon. Expected changes could include stronger regulations on data protection and privacy, including those kept or maintained by law. On the one hand, punitive measures for infringement are expected to be stricter, adhering to the law for the time being. On the other hand, more comprehensive laws to deal with all aspects of online offences are predicted. Existing bodies like the Computer Emergency Response Team (CERT) and the

[64] *Information Technology Act, No. 21 of 2000, § 66 (India)*

ISSN: 2582-6433

National Cyber Crime Reporting Portal are likely to be granted additional powers. Simultaneously, the setting up of new regulatory bodies, such as the Development Authority of India, is under consideration to provide a stronger backbone for the prevention of cyber offences, aligning with the cyber law in India. The increase in legislation that deals with cyber threats is expected to be a deterrent to criminal activity. However, an effective implementation strategy is imperative. Thus, the future of digital law will focus not just on law enforcement but also on creating an invincible, technologically adept infrastructure that can proactively identify and neutralise threats.[65]

Since cybercrime is dynamic and is a major concern, it is essential to look ahead and give the recommendations that should be made to improve electronic evidence management in India. The next includes the whole recommendations that intend to respond to the most crucial arising issues and the position to enhance the efficiency of the cybercrime inquiry.

1. Strengthening The Legal Framework

   To keep pace and technological advancements, the legal framework must be continuously regulated and updated to address new forms of cybercrime and electronic devices. Legislation should provide a clear definition in provisions for cybercrime, electronic devices admissibility and privacy concerns. There should be regular reviews. Amendments to applicable laws, such as the Information Technology Act, can ensure their continued relevance and efficacy in combating cybercrime in the current era.

2. Establishing Special Units for Cybercrime

   Predominantly, the cybercrime investigation units equipped with trained personnel and advanced technological resources should be established at the national, state, and district levels. These special units must have specialisation in electronic evidence collection, preservation, and analysis, employing digital forensics techniques.[66] Continuous training and capacity-building programs should be implemented to enhance the expertise of investigators and digital forensics professionals.

3. Promoting Private & Public Collaboration

   The collaboration between law enforcement agencies, private sector entities, public sector, academia, and civil society organisations is crucial for effective electronic evidence management. It is said that the public-private relationship facilitates the

[65] *Cyber Crime and the Law in India,* ***Delhi Lawyers.in*** *(May 27, 2024),* *https://delhi-lawyers.in/cyber-crime-and-law-india* *(last visited August 6, 2025).*
[66] *Home,* ***Ministry of Home Affairs, Gov't of India*** *(last visited August 6, 2025),* *https://www.mha.gov.in/*

ISSN: 2582-6433

exchange of ideas, knowledge, information and best practices so that the engaging technology companies, internet service providers, and financial institutions can help in proactive decision making, detection, reporting and mitigation of cybercrime.

4. Investing & Encouraging in Research & Development

   Continuous investment in research and development is critical to staying ahead of cybercriminals. Government agencies, academia, and industry should work together to create cutting-edge technology, tools, and approaches for electronic device management. Advanced data analytics, artificial intelligence, machine learning, and block chain can all be used to secure and manage electronic evidence. Promoting research and publishing case studies on cybercrime investigations and electronic evidence management can help to spread information and implement best practices.

5. Enhancing International Cooperation

   Given the global nature of cybercrime, India must strengthen its international cooperation mechanism by engaging in bilateral and multilateral agreements, mutual legal assistance treaties, and information sharing networks with other countries to promote collaborative growth. This better coordination between law enforcement organisations and international colleagues can help with cross-border investigations, electronic evidence gathering, and the extradition of cybercriminals.

6. Creating Awareness for Cyber Security

   Raising awareness about cybersecurity threats, safe online practices, and reporting mechanisms is crucial for the prevention and detection of cybercrime. With these educational campaigns targeting students, individuals, businesses, and government organisations can empower them to protect themselves against cyber threats and assist in the early identification and reporting of cybercrimes[67]. Collaboration with media outlets and social media platforms can amplify cybersecurity awareness initiatives.

The Digital Personal Data Protection Act, 2023[68]

Also known as the DPDP Act, 2023,[69] is India's attempt to bring order to how personal data is extracted and utilised, especially online. It makes consent a huge key, which basically, no one should take or use your data unless you clearly say yes. . While it doesn't directly punish

[67] *Home,* ***Ministry of Electronics & Information Technology, Gov't of India*** *(last visited August 6, 2025),* https://www.meity.gov.in/.
[68] *Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE*
[69] *Ibid*

ISSN: 2582-6433

hackers or fraudsters, it helps create a system where misuse of data is harder to get away with. The key brief concept of this act is enlisted below:

- Applicability: Digital personal data (including later-digitized data); extraterritorial if associated with products or services in India; excludes personal/domestic usage and public data.[70]
- Principles: Lawful, purpose-specific processing; minimum collection required; applies to all personal data (no sensitive or critical sub-categories).[71]
- Consent and notification: Free, informed, precise, affirmative; simple withdrawal; notification prior to consent in English or scheduled languages; pre-Act consents need notice.[72]
- Cross-Border Transfers: Allowable until blacklisted; harsher sectoral regulations apply.
- Significant Data Fiduciaries: Additional responsibilities include a data protection officer (located in India), audits, and impact assessments.
- Children/Disabled Data: Guardian consent; no damaging profiling or targeted advertising; the government may approve relaxations above a particular age.
- Data Principals' Rights: Access, correction, deletion, and nomination; must exhaust all grievance redressal options before presenting to the DPB.
- DPB: Enforces, investigates, assesses penalties, and mandates immediate action; appeals to TDSAT and the Supreme Court.[73]
- Government powers: Request information, order blockage after repeated penalties in the public interest.
- Penalties range from ₹250 crore to ₹10,000 for data breaches.[74]
- Voluntary Undertaking: Commitments may halt proceedings.
- Exemptions: Full/partial for state functions, legal claims, startups, mergers, offences, public order, sovereignty, etc.
- Legitimate uses include processing without consent for emergencies, employment, legal obligations, benefits, judgments, voluntary disclosure without opposition, and so forth.

[70] *Digital Personal Data Protection Act, No. 22 of 2023, § 4 (India)*
[71] *Digital Personal Data Protection Act, No. 22 of 2023, § 6 (India)*
[72] *Digital Personal Data Protection Act, No. 22 of 2023, § 9 (India)*
[73] *Digital Personal Data Protection Act, No. 22 of 2023, § 33 (India)*
[74] *Digital Personal Data Protection Act, No. 22 of 2023, § 39 (India)*

ISSN: 2582-6433

Conclusion

Honestly? Cybercrime today just feels... everywhere. Not just big cases or hackers, but small things too. Someone's identity stolen, a girl bullied on Instagram, fake job scams—it's hitting people hard. And the thing is, laws are *there*. Like the IT Act[75], or that new DPDP thing from 2023[76]. Sounds good. But when someone's hurt, the system? Doesn't always show up fast. Or at all.

We kept thinking: what happens *after* the crime? That part's not talked about enough. The fear people carry. How some never report anything again. We need better support, not just punishments. Cops are trained for online cases. Mental health help. Real info for people to protect themselves. That's how we move forward.

Not just more rules. More empathy. That's what we kept coming back to. Laws should protect people, not just sound strong on paper.

[75] *Information Technology Act, No. 21 of 2000, INDIA CODE*
[76] *Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE*