INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CYBER CRIME IN INDIA: LEGAL FRAMEWORK AND CHALLENGES

AUTHORED BY - ADV. SATHEESAN C.N, ADV. AADARSH PREMARAJ, ADV. AKHIL LALICHAN, ADV. PRITHVIK PRADEEP & ADV. ASHISH PAUL

Abstract

The rapid growth of information and communication technologies has transformed modern society while simultaneously giving rise to new forms of cybercrime. In India, increasing internet penetration, digital transactions, and online platforms have led to a significant rise in offences such as hacking, identity theft, cyberstalking, online fraud, and cyber terrorism. This paper examines the concept and nature of cybercrime and analyses the existing legal framework, particularly the Information Technology Act, 2000, along with relevant statutory provisions and judicial decisions. It further highlights key challenges in regulating cybercrime, including jurisdictional complexities, technological limitations in enforcement, and gaps in the current legal regime. The study argues that while India has established a foundational legal structure, it remains insufficient to effectively address emerging cyber threats. The paper concludes by suggesting the need for legal reforms, improved enforcement mechanisms, and stronger international cooperation to combat cybercrime effectively.

Keywords: Cybercrime, Cyber Law in India, Information Technology Act 2000, Cyber Security, Digital Evidence, Enforcement Challenges.

Introduction

Criminology is the scientific study of crime, criminal behavior, and society's responses to crime. It seeks to understand why crimes are committed, who commits them, and how crime affects individuals and communities. Drawing from disciplines such as sociology, psychology, law, economics, and biology, criminology examines crime as a social phenomenon rather than merely a legal violation.

Cybercrime refers to unlawful activities committed using computers, digital devices, or the internet, where technology acts as a tool, target, or medium of the offence. With the rapid

ISSN: 2582-6433

expansion of information and communication technologies, cybercrime has become a global challenge affecting individuals, businesses, governments, and financial systems. Offences such as hacking, identity theft, online fraud, cyberstalking, data breaches, and cyber terrorism threaten privacy, security, and trust in digital transactions. The borderless nature of cyberspace makes investigation and prosecution difficult, as offenders can operate anonymously across jurisdictions. In India, the growth of e-governance, digital payments, and social media has further increased exposure to cyber risks. Consequently, cybercrime demands a comprehensive response combining robust legal frameworks, advanced technological measures, skilled enforcement agencies, and public awareness. Understanding the nature and scope of cybercrime is essential for ensuring digital security and safeguarding individual rights in the modern information society.

CRIMES

Crimes are acts or omissions prohibited by law and punishable by the State. They represent behavior that threatens public order, safety, morality, and individual rights. Crimes may be committed against persons, property, society, or the State, and include offences such as murder, theft, assault, fraud, and sexual offences. The essential elements of a crime generally include a **guilty act (actus reus)** and a **guilty mind (mens rea)**, though in certain offences, strict liability applies. Modern criminal law aims not only to punish offenders but also to deter crime, reform criminals, and protect victims.

CYBER CRIME

Cybercrime refers to criminal activities carried out using computers an d the internet, targeting individuals, organizations, or government syste ms. It encompasses a wide range of activities, including identity theft, h acking, online fraud, and cyberbullying.

Cybercrime may be defined as “Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of a crime”.

Classification of Cybercrimes

Cybercrime can be generally categorized into three types: crimes against society, institutions/organizations, and individuals.

Against Society

Cybercrimes against society means when it affects the society at large.

Forgery, polluting the youngsters with indecent exposure, economic fraud, and data diddling,

ISSN: 2582-6433

sale of illegal articles, net extortion, salami attacks, cyber contraband, and logic bombs come under this category of cyber-crime. For example, forging currency notes, revenue stamps, marksheets using computers and high-quality scanners and printers.

Against Institutions/Organizations

Group of persons commit certain offences using internet facilities, intending to threaten the governmental institutions, organizations or companies, these types of offences come under the category of cybercrimes against Institutions/Organization. The main purpose of commission of these crimes are to spread terror in a particular country by circulating false information among people and creating panic among them.

Against Individuals

In this category the crime is committed against the individual or his property. When the crime is committed against the will of an individual which generally affect the individuals psychologically and creates personality disorder then such crimes are against individual. This includes harassment through emails, cyber stalking, defamation etc.

Two Main Types of Cybercrimes

Most cybercrime falls under two main categories:

- Criminal activity that *targets computers.*
- Criminal activity that *uses computers.*

In first type, the crime is done on a computer and its networks and software, like hacking into a security system, delivering a dangerous programmed, or infringement on a website title. IPR are violated when something of this nature occurs.

In the second type, a computer is a primary instrument for committing the crime, like theft, forgery, or pornographic actions. The computer was merely the tool used to commit the crime.

TYPES OF CYBER CRIMES

1. Cyber Defamation

Defamation as an act and offence has been categorically defined in Section 356(1) BNS, 2023 while Section 356(2) deals with the punishment for same. Cyber Defamation is defaming someone by harming their public image and reputation in the digital space. It typically involves the bully(ies) posting or commenting persistent destructive criticism of the victim online, on publicly accessible platforms such as social media, to create a negative, false perception of the victim in front of their contacts. It is crime committed on cyberspace through internet, with defame someone.

ISSN: 2582-6433

While the evidences of defamations and their forms are governed as per the provisions made under Section 62 and 63 of BSA 2023, Section 66A of Information Technology Act hence was made in pursuance of controlling the offence. Due to the misuse of said section 66 A of Information Technology Act, the Hon'ble Supreme Court (SUPREME COURT) in "Shreya Singhal v. Union of India"113 had struck down the said section for the fact of ambiguity in its wordings.

According to the Supreme Court advice, an individual charged with making abusive remarks on social networking websites cannot be detained if senior officers such as the IG or DCP grant their authorization

2. Cyberstalking

It is basically online harassment by one person against another person or his family by leaving threatening messages via internet. Cyberstalking is when someone uses electronic or digital means to harass or stalk a victim, such as social media, email, instant messaging (IM), or messages posted to a discussion group or forum. Cyber-stalker makes use of the anonymity feature of the internet to stalk or harass the victims without being caught, punished, or even detected.

Although cyberstalking refers to all types of online harassment, it can include slander, defamation, false charges, trolling, and even direct threats to annoy, intimidate, frighten, control, or blackmail the victim; that the private information about the victim will be revealed over the internet. A practice known as doxing is done where the information about the victim is searched for to steal their identity or perpetrate other real-world crimes, such as theft or harassment

After Megan Meier's death by suicide in Missouri in 2006, a female cyber-stalker was prosecuted and convicted in 2008 for violating the Computer Fraud and Abuse Act. Sextortion is the most common kind of cyberstalking among both kids and adolescents, as per the FBI.

In Kalandi Charan Lenka vs State of Odisha the petitioner was abused daily, and the culprit constructed a fake profile for her as well as sent indecent texts to her acquaintances in a case involving the Hon'ble Orissa High Court. Additionally, a changed indecent image was pasted on the walls of the hostel where victim slept. The court judged the culprit guilty of his crime.

3. Cyber Pornography

The use of cyberspace to publish, distribute, or design pornography is known as cyber

ISSN: 2582-6433

pornography.

Cyber pornography is known as digital sexually explicit content that is available in a variety of formats, including photographs and video files that depict naked persons and sexual content that is intended to elicit sexual enjoyment.

In India, cyber pornography is dealt under various legislative implications such as S. 67, S.67Aand 67 B of Information Technology Act 2000, Section 294 of BNS,2023, Indecent representation of women's Act 1986 and Section 13 and 14 of The Protection of Children from Sexual Abuse Act, 2012.

In Avinash Bajaj v. State of NCT Delhi122 On the website bazee.com, a user published an obscene film An F.I.R. was filed against bazee.com for selling obscene material. Avinash Bajaj, the CEO of bazee.com, was arrested by the police under Section 67 of the Information Technology Act.

4. Hacking

Hacking refers to the use of unconventional or illicit means to gain unau thorized access to a digital device, computer system, or network. While it is often associated with cybercriminal activities, such as data theft and system compromise, hacking can also be performed for ethical purpose s, such as identifying and fixing security vulnerabilities.

Types of Hackers

1. **Malicious Hackers (Black Hat Hackers)**: These individuals exploit vulnerabilities for personal or financial gain, often causing harm to indi viduals or organizations.
2. **Ethical Hackers (White Hat Hackers)**: They use their skills to help organizations improve their security by identifying and addressing vulne rabilities, often with permission from the system owners.
3. **Gray Hat Hackers**: These hackers operate in a moral gray area, break ing into systems without permission but typically to expose vulnerabiliti es rather than for malicious purposes.

Hacking Techniques

Hackers employ various techniques to exploit vulnerabilities, including:

Social Engineering: Manipulating individuals into divulging confidenti al information.

Malware: Using malicious software to gain access to systems or data.

Phishing: Sending deceptive messages to trick users into revealing sens itive information

ISSN: 2582-6433

Sending a virus by e-mail is not an illegal access. A hacker may have multiple objectives for intruding into other private spaces by making a web of scams and hence in accordance with his actions both civil and criminal liabilities may be invoked. The civil liability depends on the amount of scam, criminal liabilities may be invoked as per Section 303 of BNS and Section 75 of Information Technology Act, 2000.124.

5. Defacement of Website

Web defacement is an attack in which malevolent actors get access to a website and change the content with their own. As a result of a hacker's intrusion, the comments might include political and religious messages as well as obscenity and other unpleasant content which would embarrass the website's proprietors.

Another form of cybercrime involves the replacement of a website's original home page with a page that is libelous in nature and contains inflammatory text or unsettling imagery. Usually this is done to government or religious websites for political reasons, but corporate websites are also targeted to spoil the reputation of the company. The websites need repair after defacement and will have to be closed causing expenditure and loss to the company.

A National Health Service website that contained patient survey data was stolen by cybercriminals in 2018, according to the BBC. "Hacked by Anoa Ghost," read the defacement message.

6. Email Bombing

An email bombing attack is one in which many emails are sent to one or more electronic mails in attempt to overrun the mailbox or the server hosting the mailbox, causing it to become unavailable.

7. Email spoofing

Email spoofing is a technique used by attackers to forge the sender's add ress on an email making it appear as if it is coming from a trusted source.

Definition and Mechanism

Email spoofing involves manipulating the email header to disguise the s ender's identity. Attackers can create emails that look like they are from legitimate sources, such as a colleague, bank, or reputable organization. This is done by altering the "From" address and other header

ISSN: 2582-6433

informatio n, which most email clients display to users. Because email protocols do not inherently authenticate the sender's address, it is relatively easy for malicious actors to forge this information.

The primary motivations for doing this are to harm someone's reputation or to profit financially, for example. The Symantec Intelligence Study (Feb 2012) estimates that approximately 68 percent of all messages are spam, one in every 358.1 e-mails is fraudulent mail, and one in every

274.0 e-mails is infected with malware. It is believed that all these electronic messages were transmitted under the guise of legitimate business.

8. Data Diddling

It's illegal to change information before, during, or after it's been analyzed by a computer system, which is known as data tampering (DT) or data diddling (DD). During the writing process, recording, encoding, analyzing, verifying, translating, and transferring data, the original information can be affected by the person typing it or a virus designed to change it. It is regarded to be one of the most basic forms of computer crime. It is basically an unauthorized data alteration which is done either before or during the input of data into the computer system. This sort of crime commonly occurs in inventory system, payroll data, financial records, credit records, and other similar documents.

NDMC Electricity Billing Fraud Case, which occurred in 1996. The NDMC, Delhi, used the computer network to receive and account for electrical bills. Money collection, computerized accounting, record keeping, and bank payment were all handled by a private contractor who was a computer expert. He embezzled a large sum of money by altering data files to represent less revenues and bank payments. Section 66 (i) and 43 (d) of Information Technology Act deal with the said offence in an elaborate manner.

4.2.9 Salami Attack

The ancient "collect-the-round-off" method is used to slice salami. Mathematical routines, such as value computations, are used by the attacker. Calculations are done with decimal places, usually two or three. For instance, if we had a dollar currency, we would round to the nearest penny and ignore the remaining decimals. Without notifying the financial institution, the attacker can move these fractions of pennies to his account. It is a financial crime where the victim is the financial institutions, here an insignificant change is made which wouldn't be noticeable. For example, in banks an employee can insert a program in its servers to

ISSN: 2582-6433

automatically deduct a small amount every month from every account holder and be transferred to another account, since the amount will be very small, it will go unnoticed by the account holder, but there would be a sizeable amount in the criminal's account every month.

10 Computer Viruses/ Malwares

These are small programmes which are specially developed for corrupting or deleting data of a computer. Such viruses can be easily spread as email messages or attachments, if the attachment is opened the virus immediately gets downloaded and corrupts the programmes and data in the hard disk of that computer. Viruses are also spread when unauthorized software or files are downloaded from the internet. For example, Trojans are unauthorized programme which may be a part of an authorized programme.

There are many types of Trojans, some Trojans are destructive and may destroy the hard disk of the computer. There are also password Trojans which search for passwords in a computer system and sends it to the hacker via email.

11. Web Jacking

This is also a sort of cybercrime in which control of a website is taken over by force. The attackers do it for some monetary or political reasons. Once a web site is taken control then the actual owner of the website loses all his control, and the attacker will have full control of the website.

12. Cyber-Squatting

Cyber-Squatting is an act of registering, trafficking in or using a domain name with an intent to profit from the goodwill of a trademark belonging to someone else. Domain name sales in the name of a well-known and/or registered trademark or an ambiguously related trademark are prohibited.

In Manish Vij v. Indra Chug the Delhi High Court provided a definition of cybersquatting and described as "the act of obtaining a domain name through fraudulent registration with the goal of selling the domain name to the legitimate owner of the name for a premium."

Even though the Anti- 89 Cybersquatting Consumer Protection Act of 1999 was adopted in the US to attempt to resolve disputes in this area, there is no similar legislation in India that expressly tackles cyber-squatting. In India, all cyber-squatting proceedings are decided under Trademark Law, which is bound to be unproductive.

ISSN: 2582-6433

13. Cyber Terrorism

This is the most dreaded of all the cybercrimes which is using disruptive activities or threats in cyber space intending to intimidate people for achieving religious, political, or social objectives. Since its inception in the late 1980s, the Internet has proven to be a very flexible mode of communication, impacting an ever-increasing number of people throughout the world. In recent years, the development of increasingly complex technology has led to the formation of a network with global reach and minimal entry hurdles. Individuals can interact with complete anonymity, rapidly and effectively across geographical borders, and to a practically limitless audience because of the Internet technological capabilities.

The United Nations General Assembly strongly approved the UN Global Counter-Terrorism Strategy in 2006, signifying a significant milestone in the realm of international counter-terrorism efforts worldwide.

Under the auspices of the United Nations and its specialised agencies, including the International Civil Aviation Organization, the International Maritime Organization, and the International Atomic Energy Agency, the international community has been developing universal legal instruments to prevent terrorist acts since 1963. The universal counter-terrorist instruments are an important part of the global anti-terrorism regime and a foundation for international collaboration in the fight against terrorism.

14. Organised Criminal Groups for Committing Cybercrimes

The organised cyber-criminal groups function as legitimate businesses wherein people hired work for them as employees in various technical, administrative and support positions to complete the tasks. In the organised criminal group are two types of groups: one engages in committing *interpersonal cybercrime*s and the other group commit *cyber dependent crimes*. In the first category the members identify, recruit, and ultimately entice the victim to engage in a sex act whereas the other group needs tools and technology to commit cybercrimes. Some of them are coders, hackers, hosts, and technical support who commit crimes for a various reason, it can illegal access to systems, illegal interception or acquisition, misusing devices, data and system interface. There are also cyber enabled crimes which in ICT tools are used to commit crimes which can include traditional crimes. This type of crime includes computer related fraud and forgery, bank and payment fraud, phishing, advance fee fraud scam, romance scam (catfishing) who target people's emotions by creating fake profiles in social media and dating sites. It also includes computer related identity offences, falsified medical product related crime (use of substandard medicines) etc.

ISSN: 2582-6433

Main Causes of Cybercrimes

1. **Rapid Growth of Technology**
   Expansion of the internet, smartphones, cloud computing, and AI has increased digital dependency, creating more opportunities for cyber offenders.
2. **Anonymity in Cyberspace**
   Cybercriminals can conceal their identity using fake accounts, VPNs, and encrypted networks, making detection difficult.
3. **Lack of Cyber Awareness**
   Users often fall victim due to ignorance about phishing, malware, fake links, and unsafe online practices.
4. **Weak Security Systems**
   Poor cybersecurity infrastructure, outdated software, and lack of regular updates make systems vulnerable to attacks.
5. **Easy Access to Hacking Tools**
   Malware, ransomware kits, and hacking software are easily available on the dark web.
6. **Economic Motives**
   Financial gain through online fraud, identity theft, cryptocurrency scams, and data theft is a major driver.
7. **Inadequate Law Enforcement Capacity**
   Shortage of trained cybercrime investigators and technical experts weakens effective enforcement.

LEGAL FRAMEWORK

National

Information Technology Act, 2000

The **Information Technology Act, 2000 (IT Act)** is the primary legislation dealing with cyber crimes in India.

In the year 1999, the Information Technology Bill139 was drafted in India following the Model Law on electronic commerce which was adopted by the United Nations Commission on International Trade (UNCITRAL) in 1996 which the UN General Assembly by its resolution No. 51/162 dated 30 January 1997 had recommended to all the States to favourably consider the said Model law and enact their national laws.

Important Provisions:

- **Section 43** – Penalty for damage to computer systems, data theft

 ISSN: 2582-6433

- **Section 65** – Tampering with computer source documents
- **Section 66** – Computer-related offences (hacking)
- **Section 66C** – Identity theft
- **Section 66D** – Cheating by personation using computer resources
- **Section 66E** – Violation of privacy
- **Section 66F** – Cyber terrorism
- **Section 67** – Publishing or transmitting obscene content
- **Section 67A & 67B** – Sexually explicit content and child pornography

Information Technology Rules

The Central Government has made many rules and regulations in accordance with the authority granted by the relevant sections of the Information Technology Act 2000 as given below:

1. **Information Technology (Certifying Authorities) Rules, 2000 –** In exercise of the powers conferred by Section 87 of the Information Technology Act, 2000, these detailed rules have been made by the Central government to regulate the application and other guidelines for Certifying Authority and have described the manner in which information be authenticated by means of digital signature creation of digital signature, verification of digital signature,
2. **Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 -** In exercise of the powers conferred by Section 87 of the Information Technology Act, 2000, these detailed rules have been made by the Central government to specify the procedure for filing applications, presentation and scrutiny of applications, place of filing application, application fee, contents of application, paper book, etc. to accompany the application, plural remedies, service of notice of application on the respondents
3. **Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003–** in exercise of the powers conferred by Clauses (p) & (q) of the subsection (2) of Section 87of the Information Technology Act, 2000, the Central Government had made this rule. This rule specifies the eligibility of the adjudicating officer, the scope and manner of holding inquiry, the factors the adjudicating officer needs to follow before passing an order, certified copies of orders, service of notices and orders, the specified fee with the applications.
4. **The National Cyber Security Policy** is a growing task which caters to the whole ambit of ICT users including small and large institutions. It is a vision that is integrated and

ISSN: 2582-6433

has a set of strategies which are sustained and coordinated for execution. The objectives and execution plans are fully integrated. It will be of use like umbrella framework for guiding and defining the cyber security in cyberspace. The policy gives an over-view of Government's approach and plan for protecting cyberspace in the country. One of the important objectives of the policy is to straighten the regulatory framework for assuring a secured cyberspace ecosphere.

Data Protection Law in India.

5. The right to privacy in India was declared a fundamental right by the Hon'ble Supreme Court of India on 24 August 2017, in its landmark judgment in the case of *Justice K.S. Puttaswamy (Retd.) v. Union of India ("**Right to Privacy Case**").167 After this case, the need was felt to have a stronger legislation in place to protect the personal data and privacy of individuals. Accordingly, in August 2017, the Central Government appointed a data protection committee chaired by retired Supreme Court Judge, **Justice B N Srikrishna,** on 27 July 2018, the committee released an extensive **white paper**168 on the importance of data protection. Subsequently in July 2018, the committee released the draft Personal Data Protection Bill, 2018.*

International Law

International Conventions & Protocols

1. The Council of Europe in the year 2001 had initiated Convention of Cybercrime which is one of the most important international initiatives to develop criminal law, it is also called as Budapest Convention.171 Many members States of Council Europe and some other countries have ratified this. A common minimum standard of relevant crimes has been established by this convention and it is the only binding instrument on cybercrimes that have been adopted. In these nine different types of cybercrimes which involves human acts and computer networks. The States who are part of this convention have agreed to include these nine types of cybercrimes in their domestic laws, a list of valid practices is also provided

2. The UNCTAD Worldwide Cyber law Tracker 174is the world's first international mapping of cyber laws and is being developed in collaboration with the World Bank. It keeps track of the current level of electronic commerce laws in the areas of electronic transactions, consumer rights, privacy laws, and cybercrime implementation in the 194 member countries of the United Nations Conference on Trade and Development. It

ISSN: 2582-6433

displays whether a specific country has passed legislation, or whether a draft law is currently being considered for passage. When information on a country's legislative adoption is not readily available, the phrase 'no data' is used to signify that no information is available.

3. The Hanoi Convention on Cybercrime, also known as the United N ations Convention against Cybercrime, is a landmark international treaty adopted by the General Assembly of the United Nations on December 24, 2024. It aims to strengthen international cooperation in combating cybercrime and is the first comprehensive global trea ty on this matter. The Convention provides States with a range of measures to prevent and combat cybercrime and aims to strengthen international cooperation in sharing electronic evidence for serious crimes. It will remain open for signature until December 31, 2026, and will enter into force after 40 States become Parties. The Conv ention is expected to facilitate the collection, preservation, sharing, and use of electronic evidence across borders, addressing the challe nges of inconsistent national laws and slow mutual legal assistance procedures.

   United Nations Convention Against Cybercrime

4. The United Nations Convention against Cybercrime aims to strengthen global cooperation to address crimes committed through information and communications technology (ICT) systems. As cyber-enabled offenses grow more sophisticated, the Convention seeks to harmonize legal frameworks, promote capacity-building, and enhance mechanisms for timely cross-border assistance. A key objective is facilitating secure and efficient sharing of electronic evidence related to serious crimes, ensuring that jurisdictions can act quickly despite differing legal systems. The Convention encourages states to adopt compatible procedures for preservation, disclosure, and exchange of digital data while upholding human rights and due process. By improving coordination among law-enforcement agencies, fostering technical collaboration, and supporting developing countries in building cyber-resilience, the Convention represents an important step toward a unified global response. Ultimately, it aims to ensure that cybercrime is effectively investigated and prosecuted worldwide, reducing safe havens and strengthening international security.

Current Initiatives at the International Arena

The United Nations General Assembly in tis 74th session adopted resolution no. 74/247 on 27 December 2019 for countering the use of ICT for criminal purposes. Pursuant to the said

ISSN: 2582-6433

resolution, the ad hoc committee was convened for agreeing on outline and modalities of future activities which was required to be submitted to the UNGA in the 75th session. The General Assembly on 26 May 2021, they adopted resolution 75/282 which was titled "*Countering the use of information and communications technologies for criminal purposes*."

Preventive Measures Against Cybercrimes

1. **Strong Cyber Laws and Enforcement** Effective implementation of laws like the Information Technology Act, 2000 and coordination with BNS and BNSS provisions.
2. **Public Awareness and Education** Regular awareness programs on safe online behavior, password security, and recognizing cyber fraud.
3. **Use of Advanced Security Measures** Firewalls, antivirus software, encryption, two-factor authentication, and regular system updates.
4. **Capacity Building of Law Enforcement** Training police and judicial officers in cyber forensics and digital evidence handling.
5. **International Cooperation**
   Cross-border collaboration through treaties and conventions to address transnational cybercrime.
6. **Responsible User Behaviour** Avoiding suspicious links, using strong passwords, securing personal data, and reporting cyber offences promptly.

Cybercrime rates in India (latest statistics):

National Trends

- In **2023**, India recorded **86,420 cybercrime cases**, up **31.2% from 2022** (65,893 cases).
- The **crime rate** (cases per lakh population) rose from **4.8 in 2022 to 6.2 in 2023**.
- *Fraud* accounted for about **69% of all cybercrime cases**. **Reporting Portal Data**
- The **National Cybercrime Reporting Portal (NCRP)** logged **millions of complaints**; on average thousands per day, with increasing FIR conversions.
- India saw about **129 cybercrime incidents per lakh population in 2023**.

State & City Variation

- **Delhi** had one of the highest cybercrime complaint rates per population.
- **Karnataka, Telangana, and Uttar Pradesh** reported the highest absolute numbers of cases.

ISSN: 2582-6433

Financial Impact

- Government data show **cyber fraud losses escalating** (e.g., ₹22,845 crore in 2024, a large jump from 2023).

Overall, cybercrime in India is rising rapidly due to expanded internet use, digital payments, and more online services, making it a major concern for law enforcement and users alike.

Some judgements relating to Cyber law and Cybercrime Google India Private Limited vs Visaka Industries

In this case there was complaint against appellant Google India that it became a party to a defamatory act under Ss. 499 and 500 IPC, by not taking down an allegedly defamatory post uploaded by one of its users on Google Groups despite this being brought to Google India's notice. It was held by the Court that original S.79 of Information Technology Act because of its narrow scope did not come to Google India's aid.

Ghulam Nabi Azad vs Union of India

Present case involving abrogation of Article 370 of Constitution of India (pertaining to temporary provisions as to State of Jammu and Kashmir). The government suspended internet services, phone networks, etc. in the State of Jammu and Kashmir stating it to be a preventive measure taken to avoid any danger to national security having regard to background and history of said State facing terrorism for past many years. It was held that under S.69-A of IT Act, 2000 is limited as the aim to that provision is not to block the internet but only to block access to websites on internet, hence recourse cannot be made by government to restrict the internet generally under S.69- A.

Amit Sahni vs Commissioner of Police

After the Citizenship (Amendment) Act, 2019 was passed, its constitutionality was challenged by filing a writ petition under Article 32 of the Constitution by a section of the society in the Supreme Court of India. When freedom of speech and expression/Right to protest are expressed through social media channels, the ability to scale up quickly using digital infrastructure. The Supreme Court observed that the social media channels often fraught with danger and can lead to the creation of highly polarised environments.

ISSN: 2582-6433

Manik Taneja vs State of Karnataka

Being aggrieved with the manner with which they were treated by the police in regard to a traffic accident, the appellants posted comments on the Bangalore Traffic Police Facebook page, accusing the Inspector concerned of his misbehaviour and also forwarded an email complaining about the harassment meted out to them at the hands of the respondent Police Inspector.

The Court held that Facebook, a social networking is a public forum, and it facilitates expression of public opinion. Posting of one's grievances against the government machinery, even on government Facebook page does not by itself amount to criminal conduct.

Kamlesh Vaswani vs Union of India

Crimes against women and children like pornography on internet. It was held that innocent children cannot be made prey to these kinds of painful situations and a nation, by no means, can afford to carry any kind of experiment with its children in the name of liberty and freedom of expression. A Cyber Regulation Advisory Committee was constituted under S.88 and inter alia, assigned with brief regarding availability of pornography on internet.

The Government blocked many websites under provision of Section 79
(3) (b) of the Information Technology Act, 2000 as content hosted on those websites relate to morality, decency as given in Article 19(2) of the Constitution of India.

State vs Amit Prasad 2009

The case of State vs. Amit Prasad was the first hacking case to be filed in India under Section 66 of the Information Technology Act 2000. This case, which had its own set of facts, highlighted how well the provisions of Indian Cyber Law might be read in a variety of ways, based on whose side of the criminal investigation you were on.

China executes 11 people tied to Myanmar scam compounds

China has executed 11 people who were convicted of being part of criminal gangs in Myanmar, including "key members" of telecom fraud operations, Chinese state media reported on Thursday.

The 11 were found guilty and sentenced to death in September by a court in Wenzhou, in China's eastern Zhejiang province

Executed for murder, illegal detention, fraud and gambling

The executed criminals included members of the "Ming family criminal group," state media

ISSN: 2582-6433

said. They were sentenced to death "for crimes including intentional homicide, intentional injury, illegal detention, fraud and operating gambling establishments," Xinhua reported.

The 11 criminals had been found guilty of having "established multiple operational bases in Myanmar to engage in telecom fraud, operate illegal gambling dens and commit other crimes" in operations dating back to 2015.According to the Supreme People's Court (SPC), which reviewed the case after the 11 defendants appealed the verdict, the funds involved in the fraud operations and gambling exceeded 10 billion yuan (around

€1.2 billion or $1.4 billion)."The gangs also intentionally murdered, assaulted, and illegally detained people involved in fraud, resulting in the deaths of 14 Chinese citizens and causing injuries to others," Xinhua reported.

What do we know about the scam compounds in Southeast Asia?

Scam compounds have thrived in Southeast Asian neighbors Thailand, Cambodia and Myanmar, particularly in the latter's lawless border areas.The scam centers, which are part of a multibillion-dollar illegal industry, are usually staffed by foreigners, including Chinese nationals.

Many of them claim they were trafficked and forced to work at the centers, scamming people online.

In recent years, Beijing has increased its collaboration with Southeast Asian countries to clamp down on the scam centers.

How to file a Cybercrime complaint online in India?

A cybercrime complaint can be filed using the National Crime Reporting Portal of India.

Website link is – https://cybercrime.gov.in/

National Cyber Crime Reporting Portal of India

This portal is an initiative of the Government of India to facilitate victims/ complainants to report cybercrime complaints online.

This portal caters for all types of cybercrime complaints including complaints pertaining to

- online Child Pornography (CP),
- Child Sexual Abuse Material (CSAM),
- sexually explicit content such as Rape/Gang Rape (CP/RGR) content and
- other cybercrimes such as mobile crimes, online and social media crimes, online financial frauds, ransomware, hacking, cryptocurrency crimes and online cyber

ISSN: 2582-6433

trafficking.

The portal also provides an option of reporting an anonymous complaint about reporting online Child Pornography (CP) or sexually explicit content such as Rape/Gang Rape (RGR) content.

Cybercrime Helpline Number

The Cyber Crime Helpline Number is 155260.

Indian Computer Emergency Response Team (CERT-IN or ICERT)

The **Indian Computer Emergency Response Team** (**CERT-IN** or **ICERT**) is an office within the Ministry of Electronics and Information Technology of the Government of India.

Conclusion

Cybercrime has emerged as a significant challenge in the digital era, driven by rapid technological advancement and increasing dependence on online platforms. In India, the rise in cyber offences highlights both the opportunities and vulnerabilities created by digital transformation. The Information Technology Act, 2000, along with judicial developments such as Shreya Singhal v. Union of India, provides a foundational legal framework to address cybercrime. However, the evolving nature of cyber threats, including sophisticated online frauds, data breaches, and transnational crimes, exposes the limitations of existing laws.

The study demonstrates that while the legal framework is comprehensive in scope, its effectiveness is hindered by enforcement challenges, jurisdictional complexities, and lack of technical expertise. There is a pressing need to modernise cyber laws to keep pace with emerging technologies, strengthen institutional capacity, and enhance coordination at both national and international levels.

A proactive and adaptive approach, combining legal reform, technological advancement, and public awareness, is essential to combat cybercrime effectively. Only through such a comprehensive strategy can India ensure a secure digital environment and maintain public trust in the rapidly expanding digital ecosystem.