CYBER OFFENCES:
Issuses Challenges & Solutions

Reading Material

23rd February, 2025

Prepared by :
Judicial Academy, Jharkhand

Judicial Academy Jharkhand

Cyber Crime Cases: Issues, Challenges & Solutions

Reading Material

For

State-Level Conference on Speedy & Qualitative disposal of Cyber Crime Cases: Issues, Challenges & Solutions

23rd February, 2025

Prepared by :

Judicial Academy, Jharkhand

Near Dhurwa Dam, Dhurwa, Ranchi – 834004

Phone : 0651-2772001, 2772103, Fax : 0651-2772008

Email id : judicialacademyjharkhand@yahoo.co.in, Website : www.jajharkhand.in

DISCLAIMER

- This book is intended for Private Circulation Only.
- The information contained in this book is intended for information purposes only and should not be construed as legal advice on any subject matter.
- The cases and content provided are for educational purposes and illustrative understanding. For a comprehensive understanding, readers are encouraged to refer to the complete case laws and official sources.
- The government schemes, sections, and rules mentioned in this book are intended solely for professional understanding. For complete and authoritative information, readers are advised to refer to the relevant Bare Acts and official legal documents.

Justice
Rongon Mukhopadhyay
Judge,
High Court of Jharkhand
Cum-Judge-In-Charge,
Judicial Academy, Jharkhand

MESSAGE

"Technology trust is a good thing, but control is a better one."
Stephane Nappo

It gives me immense pleasure to share a few thoughts on the publication of this study material on *Cyber Crimes and their Legal Framework* by the Judicial Academy, Jharkhand. In an era where technology is deeply embedded in our daily lives, the rise of cyber crimes poses unprecedented challenges to individuals, businesses, and law enforcement agencies. Understanding the complexities of digital offenses and the evolving legal landscape is essential for ensuring justice and maintaining the integrity of cyberspace.

This study material provides an in-depth analysis of cyber crimes, relevant legal provisions, investigation techniques, and judicial perspectives. By covering critical topics such as hacking, financial fraud, cyber stalking, and digital evidence, it serves as a comprehensive guide for judicial officers, legal practitioners, and law enforcement personnel. Additionally, the inclusion of landmark judgments and case studies offers valuable insights into the practical application of cyber laws.

I commend the Judicial Academy, Jharkhand, for its dedication to knowledge dissemination and capacity-building in this crucial domain. As we navigate the digital age, let us collectively work towards strengthening our legal responses to cyber threats while upholding the principles of justice and fairness.

Warm regards,

Justice Rongon Mukhopadhyay

Acknowledgement

The Judicial Academy, Jharkhand takes immense pride in presenting this book titled *"Cyber Crime: Issues, Challenges and Solutions."* This book is a comprehensive compilation of the legal, technical, and procedural aspects of cybercrime, aiming to serve as a valuable resource for judicial officers, law enforcement agencies, legal professionals, and researchers. It delves into the various types of cyber offenses, investigative procedures, digital evidence, and emerging challenges in the field of cyber law.

The Academy extends its heartfelt gratitude towards His Lordship **Hon'ble Mr. Justice Rongon Mukhopadhyay, Judge, High Court of Jharkhand cum Judge In-charge, Judicial Academy Jharkhand,** for the unwavering support and encouragement in bringing this book to fruition. His Lordship's vision and guidance have been instrumental in the successful completion of this work, and for that, the Academy shall remain eternally grateful.

We also express our sincere gratitude for valuable insights and interest of **Shri Manoj Prasad, Registrar General, High Court of Jharkhand,** for his continuous support and encouragement throughout the process.

This compilation is the result of the dedicated efforts of **Sri Laxmi Kant – Additional Director-II cum Senior Faculty Member, Judicial Academy, Jharkhand; Sri Amikar Parwar – Administrative Officer;** and the **Research Scholars – Ms. Jyotsna Singh, Ms. Sarita Akhuli, Mr. Harsh Mishra and Mr. Uday Narayan.** Their persistent efforts, meticulous research, and commitment to this book have been invaluable in shaping this book into a comprehensive and insightful resource.

We sincerely hope that this book will provide meaningful insights and serve as an additional-practical piece of information for all stakeholders involved in addressing and combating cybercrime.

Satyakam Priyadarshi
Director In- Charge
Judicial Academy, Jharkhand

Table of Contents

List of Abbreviations

AI	Artificial Intelligence
ATM	Automated Teller Machine
BNS	Bharatiya Nyaya Sanhita
BNSS	Bharatiya Nagarik Suraksha Sanhita
BSA	Bharatiya Sakshya Adhiniyam
C.D	Compact Disc
CrPC	Criminal Procedure Code
CSEAM	Child Sexual Exploitation and Abuse Material
CVV	Card Verification Value.
FIR	First Information Report
FSL	Forensic Science Laboratory
HC	High Court
I.O	Investigating Officers
I4C	Indian Cybercrime Coordination Centre
IPC	Indian Penal Code
IT Act	Information Technology Act
NCMEC	National Centre for Missing & Exploited Children
NCRB	National Crime Records Bureau
OTP	One Time Password
PIN	Personal Identification Number
POCSO	Protection Of Children from Sexual Offences
PSB	Problematic Sexual Behaviors
SC	Supreme Court
SIM	Security Information Management
SMS	Short Message Service
v./vs.	Versus

Chapter 1: Cyber Crime and Types

1.1 INTRODUCTION

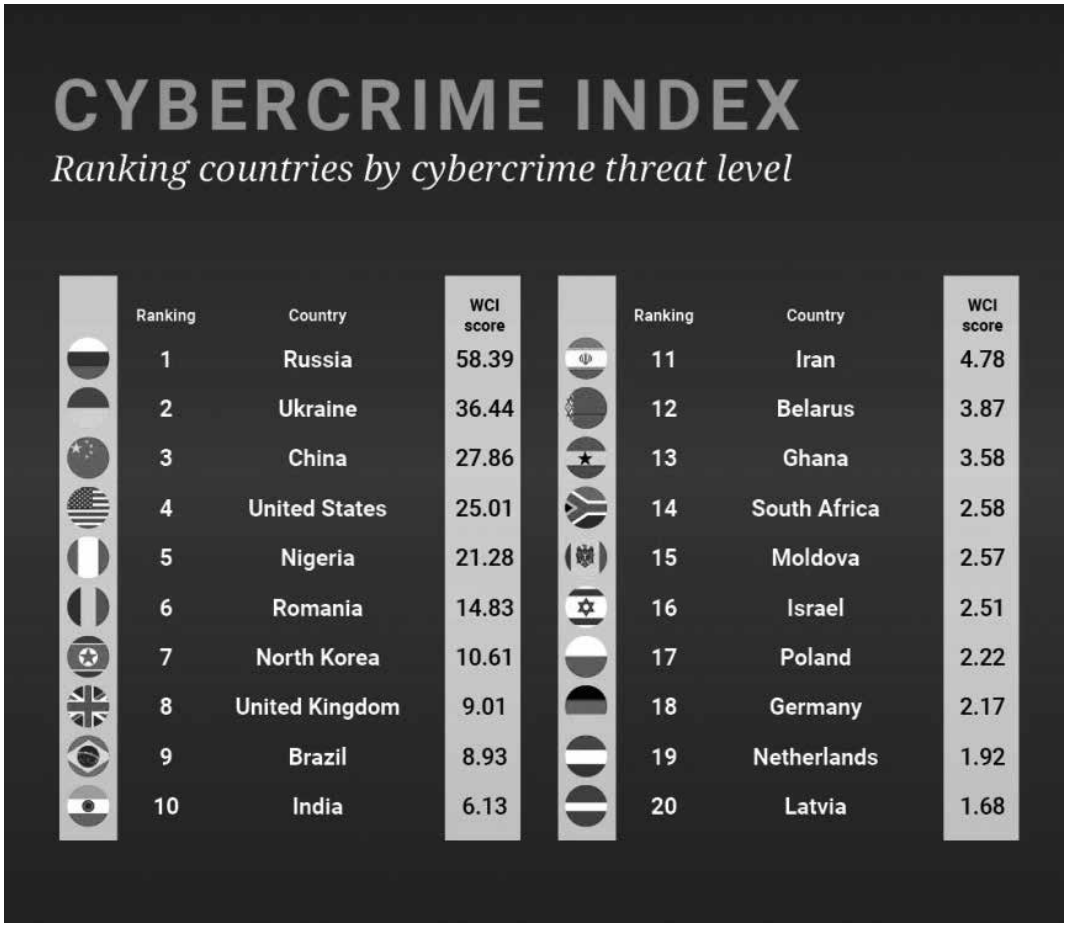
Cyber crime is a modern and pervasive issue that involves criminal activities conducted through computers, internet, or other related technologies. It is a growing threat in India, where criminals exploit the anonymity provided by technology. Cyber crime encompasses a wide range of illegal activities, including cyber-stalking, cyber-terrorism, email spoofing, cyber pornography, and cyber-defamation, as well as traditional crimes committed online. Although cyber crime is not explicitly defined in Indian legislation, it is broadly understood as any illegal act where computers or the internet is either a tool or a target. As dependence on digital technology increases, so does the potential for misuse, making cyber crime an uncontrollable menace that requires urgent attention and regulation.

Definition:

The laws don't provide the exact definition of Cyber crime, even the Information Technology Act, 2000; which deals with cyber crime doesn't define the term of cyber crime. However in general the term cybercrime means any illegal activity which is carried over or with the help of the internet or computers.

Cyber Crime Rate:

An international team of researchers has compiled the 'World Cybercrime Index' that ranks roughly 100 countries and identifies key hotspots according to various categories of cybercrime, including ransomware, credit card theft and scams. In this ranking, India ranks at number 10 in cybercrime.



The year 2024 has marked a new high in cyber crimes in India. As per data, the number of average complaints has increased to 7000 per day. This number is around **113.7%** more in comparison to 2021–2023 and **60.9%** higher than 2022–2023. In just the first 4 months, around **7,40,000 cases** were registered on the Cyber Crime portal, and this number surged to **12 lakh** by September 2024. Beyond the shocking case numbers, there are huge losses of capital too. Victims have collectively lost over **₹120 crores** to cyber frauds in the first nine months of 2024 alone. This depicts that **cybercrime in India** is increasing significantly, demanding immediate attention and action.

While rising cybercrime cases have become a cause for concern for the Centre, out of the total 1.67 lakh cases registered between 2020-2022 in all 28 states, only 2,706 persons (1.6%) have been convicted under these offences.[1]

1 https://www.tribuneindia.com/news/delhi/only-1-6-conviction-rate-in-2-yrs-amid-surge-in-cybercrime-cases/

Rising Statistics of cyber offences against women and children

Recent data from the National Crime Records Bureau (NCRB) highlights the alarming trend of increasing cyber crimes against both women and children. The statistics reveal a staggering 32% rise in cyber crimes against children from 2021 to 2022, with over 19,000 cases reported in 2022, a significant portion involving online sexual exploitation and abuse. Similarly, crimes against women have also seen a notable increase, with a 4% rise in overall cases reported in the NCRB 2023 report. This increase underscores the urgent need for effective measures to safeguard these vulnerable populations in the digital landscape.

Legislative Framework

To combat these rising threats, India has established a robust legal framework aimed at protecting both women and children from cyber crimes. Key legislations include.

The Information Technology Act, 2000	This act addresses various cyber crimes and provides guidelines for the protection of individuals online.
Bharatiya Nyaya Sanhita 2023	Certain sections of the BNS are applicable to offenses against women and children, including those related to sexual offenses and exploitation.
Protection of Children from Sexual Offences (POCSO) Act, 2012	This act specifically aims to protect children from sexual abuse and exploitation, providing a comprehensive legal framework for the prosecution of offenders.
The Protection of Women from Domestic Violence Act, 2005	This act aims to protect women from domestic violence, including emotional and psychological abuse that can occur in digital spaces.
The Indecent Representation of Women (Prohibition) Act, 1986	This act prohibits the indecent portrayal of women in various media.

1.2 CYBER OFFENCES EXPLICITLY IDENTIFIED UNDER IT ACT, 2000

Cyber Offences under the Information Technology Act, 2000 as amended in 2008 have not been defined in the Act explicitly but have been categorised. Cyber offences are usually generalised into three categories that are the ones committed against person, property and the government. Chapter 11 of the Act covers the offences and the Penalties that are accrued upon when the law is threatened. The cyber offences as mentioned under the Information Technology Act, 2000 have been delineated below:

1.2.1 IDENTITY THEFT (SECTION 66C)

It happens when a person steals your personal information—such as your Aadhaar card Number, bank account number, and credit card information. Identity theft is committed in various different ways. The increase in digital interactions and dependence on technology has created a favourable ground for cybercriminals to exploit vulnerabilities. Identity theft can lead to substantial financial losses, damage one's reputation, and cause emotional distress. It disrupts individuals' lives, hampers businesses' operations, and erodes trust in online platforms.

Section 66C of the IT Act prescribes punishment for identity theft which is imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

1.2.2 IMPERSONATION (SECTION 66D)

A person is said to commit an act of personation if he cheats by pretending to be some other person or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such person as defined under section 319(1) of Bharatiya Nyaya Sanhita 2023.

Section 66 D of IT Act prescribes the punishment for the offence of impersonation using electronic means, i.e. imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

1.2.3 VIOLATION OF PRIVACY (SECTION 66E)

In the realm of internet, now a days even the offences like vouyerism is now being perpetrated through internet and can be broadly mentioned as cyber vouyerism.

Section 66E of the Information Technology Act, 2000 addresses the issues of electronic voyeurism and bodily privacy. This section complements existing provisions in the Indian Penal Code (IPC), such as sections 292 and 509, but is more comprehensive and is gender-neutral.

While Section 354C of the IPC addresses voyeurism (focusing on women), it is gender-specific. Section 66E, on the other hand, addresses voyeurism in a broader context, prohibiting the capturing, publishing, or transmitting images of a person's private area without their consent in circumstances violating their privacy.

This law responds to the rise of **electronic voyeurism**, fueled by the widespread availability of smartphones with cameras. It criminalizes the act of capturing or sharing such images and mandates a **punishment of up to 3 years imprisonment**, or a **fine of up to ₹2 lakhs**, or both.

1.2.4 CYBER TERRORISM (SECTION 66F)

The Section 66F of the Information Technology Act[2] addresses cyber terrorism. It was added in 2008 with various changes. These changes are the result of the well-known 26/11 terror attack. Section 66F of the *Information Technology (Amendment) Act, 2008* defines and provides punishment for cyber terrorism.

1.2.5 HACKING (SECTION 45, 63 & 66)

Hacking refers to gaining unauthorized access to someone else's computer, similar to phone-tapping, by exploiting weaknesses in the computer's security. Hackers identify vulnerabilities in a system and find ways to infiltrate it. There are several tools like firewalls and intrusion detection systems which are used for prevent hacking.

2 **Section 66F. Punishment for cyber terrorism.**
(1) Whoever,--
(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by--
(i) denying or cause the denial of access to any person authorised to access computer resource; or
(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
(iii) introducing or causing to introduce any computer contaminant,
and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or
(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,
commits the offence of cyber terrorism.
(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Hacking per se, in simple terms, is akin to criminal trespass[3] into a computer, which is private property. Hacking, in its various forms, often serves as a means to commit other crimes, such as cheating, theft, misappropriation, criminal breach of trust, espionage, or even conspiracy to wage war against the State.

Initially, the title of Section 66 was misnomer, which created confusion. It was widely believed as if Section 66 was the only legal provision that dealt with the offence of hacking a computer system. This confusion has been successfully done away with, by certain amendments made by the I.T. (Amendment) Act, 2008. The words "Hacking with Computer System" have been deleted from Section 66, the scope of which has been substantially widened.

Various forms of commonly recognised hacking are mentioned below:

White hat hacker

A White hat hacker is a person who has been employed by an organization to look for loopholes in their security systems and patch the vulnerabilities of the system, before a security breach happens. White hat hackers are often behind the scenes, thwarting attacks in real time, or proactively exposing weakness to try to help keep services running and data protected.

Black hat hacker

A Black hat hacker is an Individual who tries to break into a website or security networks of an organization, unauthorized and with malicious intentions. Their primary motivation is usually for personal and financial gain, but they can also be involved in cyber espionage, protest or perhaps are just addicted to the thrill of cybercrime.

Grey hat hacker

Grey hat hackers are a blend of both black hat and white hat activities. Grey hats exploit networks and computer systems in the way that black hatside, but do so without any malicious Intent, disclosing all loopholes and vulnerabilities to law enforcement agencies or intelligence agencies Grey hats may also extort the hacked, offering to correct the defect for a nominal fee.

3 Criminal trespass under the Bharatiya Nyaya Sanhita, 2023 is defined as entering into property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, by unlawfully remaining there with intent thereby to intimidate, insult or annoy any such person or with intent to commit an offence.

1.2.6 CYBER PORNOGRAPHY

Cyber pornography refers to the use of cyberspace to create, display, distribute, or publish pornographic or obscene materials. With the rise of digital media, traditional forms of pornography have been largely replaced by online content. However, there is no universal or legal definition of pornography, as its meaning is shaped by societal norms, values, and cultural standards, which vary widely across countries and time periods. Indian law does not provide a specific definition for pornography or address it directly. The word 'Pornography' has not been defined legally in any part of the world. The basic reason behind this is very simple; neither is there any uniform standard of moral culture, values and ethics and nor there are uniform standard of law.

Also, the terms "obscenity" and "pornography" are related but distinct, and materials banned in some countries may be permissible in others. To understand the gravity and effect of pornography and obscenity on society, we need to understand these terms in their widest possible amplitude. There have been judicial pronouncements wherein some test have been mentioned to identify the presence of obscenity. A basic understanding of these are necessary as obscenity and pornography may be distinct but somewhere they overlap also.

Tests:

Hicklin Test	The test of obscenity was first laid down in the case of *Regina v. Hicklin (1868)* as the tendency "to deprave and corrupt those whose minds are open to such influences and into whose hands a publication of this sort may fall", and it was understood that this test would apply only to the isolated passage of the work.
American Roth Test	The Supreme Court of United States in the case of *Roth v. United States (1997)* created a new test for courts to determine whether something was unlawfully obscene. In this test the target was an average person, applying community standard which means that the material should be taken as a whole to consider something is obscene or not.

Miller Test	In *Miller v. California (1973)*, the Supreme Court of United States overturned the Roth test and gave the basic guidelines and three point tests to determine obscenity in the work i.e. 1. That the average person, applying contemporary "community standards", would find that the work, taken as a whole, appeals to the prurient interest. 2. That the work depicts or describes, in an offensive way, sexual conduct or excretory functions, as specifically defined by applicable state law or applicable law. 3. Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.
Community standards test	*This test applicable in India.* The Community Standards Test says that the act or any gesture or content is obscene only if the dominant theme taken as a whole is opposed to contemporary community standards

Indian Perspective

In the landmark judgment of *Ranjit Udeshi v. the State of Maharashtra* (1964) the Supreme Court adopted the Victorian-era Hicklin test. The test assessed obscenity by the standard of an individual who was open to immoral influences and would likely to be corrupted or depraved by the material in question.

The scope of obscenity has been significantly reduced by the judicial pronouncements over the years. In the *Aveek Sarkar v. The State of West Bengal* (2018) the Supreme Court did not apply the British Hicklin test and used the American Roth test instead. As per this test, obscenity was to be evaluated from an average person's perspective, applying prevailing community standards. The contemporary community standards test takes into account the changing values in society and how something which could be considered obscene ten years back would not be considered obscene today.

Indian Laws

In India, the Bharatiya Nyaya Sanhita,2023 (BNS) also prescribes punishment for obscenity. However, with the evolution of internet technology, obscenity and pornography takes electronic form and it becomes very difficult to meet the challenges through traditional laws. To deal with this, the Government of India has enacted Information Technology Act 2000. Section 67 & 67A

of Information Technology Act, 2000; prescribes punishment for obscenity and pornographic content on the internet.[4]

The Hon'ble Supreme Court in ***Sharat Babu Digumarti v. Govt. of NCT of Delhi*, (2017) 2 SCC 18** held that Chapter XI of the IT Act, more particularly Section(s) 67 through 67B are a complete code in itself when it comes to offences relating to electronic forms of obscene and pornographic material. Thus, Section(s) 67, 67A and 67B of the IT Act being a complete code, ought to be interpreted in a purposive manner that suppresses the mischief and advances the remedy and ensures that the legislative intent of penalizing the various forms of cyber-offences relating to children and the use of obscene/pornographic material through electronic means is not defeated by a narrow construction of these provisions.

Child Pornography:

It is the representation of a child engaged or involved in real or simulated explicit sexual activities in audio, video, or written form through various means like electronic, digital, optical means. It involves the use of a minor in sexually explicit conduct. It can also be the case where the visual depiction has been created, adapted, or modified to make it appear that a minor is engaging in sexual conduct. It is nothing but a child's sexual abuse and exploitation of children engaged in such activity which directly hamper their well-being, and harm their physical as well as mental health.

In any case involving child pornography, the definition of "child" under Section 2(1)(d) of the POCSO Act is less important than the definition of "child pornography" under Section 2(1)(da) of the POCSO Act. Therefore, when the court is dealing with an offence of child pornography, it must focus on the definition of "child pornography" as outlined in Section 2(1)(da), not the definition of "child" in Section 2(1)(d). In other words, the key consideration for invoking Sections related to child pornography is the definition of "child pornography."

4 **Section 67 of the IT Act provides:**
"Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.
Section 67A of the IT Act provides:
"Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees."

Children are vulnerable due to easy internet access. Pedophiles exploit them through manipulation, false promises, and monetary offers, leading to severe emotional and psychological harm.

How do they operate?

1. Pedophiles use false identity to trap the children/teenagers
2. Pedophiles contact children/teens in various chat rooms which are used by children/teens to interact with other children/teens.
3. Befriend the child/teen.
4. Extract personal information from the child/teen by winning his confidence.
5. Gets the email address of the child/teen and starts making contacts on the victim's email address.
6. Starts sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his inhibitions so that a feeling is created in the mind of the victim that what is being fed to him is normal and that everybody does it.
7. Extract personal information from child/teen
8. At the end of it, the pedophiles set up a meeting with the child/teen out of the house and then drag him into the net to further sexually assault him or to use him as a sex object.

Legal Aspects in India

Protection Of Children from Sexual Offences (POCSO) Act, 2012 Act was enacted to provide a robust legal framework to protect children from sexual assault, sexual harassment, and The procedure of this act has been designed to insure operation of this law in best possible child friendly manner. In the year 2019 the POCSO Act was made more robust by enhancing quantum of punishment as well as by defining child pornography in section 2(da) which means any visual depiction of sexually explicit conduct involving a child which include photograph, video, digital or computer generated image indistinguishable from an actual child and image created, adapted, or modified, but appear to depict a child. The Act defines child pornography as any visual representation of sexually explicit behaviour involving a child, including photographs, video, digital or computer generated images that cannot be distinguished from a child.

Further Information Technology Act, 2000 punishes the publishing or transmission of any obscene material in electronic form as well. Initially the Act did not had any specific provisions regarding child pornography; all the instances of pornography were dealt under Section 67 of

the Act. It is important to note that the IT Act, 2000 was an important step forward over the then existing laws such as ***Indian Penal Code 1860 and the Indecent Representation of Women (Prohibition) Act 1986***. The subsequent amendment to the IT Act in the year 2008 prescribes specific punishment for the child pornography. The act of publishing or transmitting material depicting children in sexually explicit behaviour is made punishable. Moreover, it also punishes browsing, collection, distribution, and creation of any sexually explicit material containing children. Inducing online relationship with children with an intention to extract sexual benefits, facilitating online child abuse and recording sexual abuse of children in electronic form is now also a punishable offence. The Act provides for a punishment with an imprisonment of five years and a fine up to five lakhs rupees and the second conviction is punishable with an imprisonment of seven years and a fine up to ten lakhs rupees. The offence made under the Act is non-bailable and cognizable.

Even after having such elaborate legal provisions punishing child pornography, curtailing child pornography is a challenging task. The present technology is not so developed to churn out child pornography from the wide area of pornography. Though the provisions has been enacted under the different statutes but the problem remains of its implementation and is a serious issue since in the physical world the implementation can be possible due to stricter approach by the government but as for the digital sphere is concerned, the Government seems to have concern of technological challenges that exists for the Government and even these institutions who are accorded with the duty to do so are not even funded properly, so in actually to curb the problem a serious approach is required.

In the year 2024, an important issue came before the Hon'ble Supreme Court regarding the contours of child pornography, including its storage, possession, and presumptions associated with it. This matter was considered in the case of *Just Right for Children Alliance v. S. Harish* (2024 SCC OnLine SC 2611)

Just Rights For Children Alliance v. S. Harish (2024 SCC OnLine SC 2611)

Facts

On January 29, 2020, the Cyber Tipline Report of the NCRB informed Tamil Nadu police that the accused, S. Harish was consuming CSEAM (child sexual exploitation and abuse material)[5], which is often referred to as child pornography under the POCSO Act. The investigation revealed that Harish had downloaded material depicting children in sexual acts on his mobile

5 The Hon'ble SC recommended that the Courts should use the term "child sexual exploitation and abuse material" (CSEAM) instead of "child pornography" in all judicial orders and judgments.

phone. Subsequently, an FIR was registered against him under Section 67B of the IT Act[6] and Section 14(1) of the POCSO Act. Section 67B of IT Act prescribes punishment for publishing or transmitting material depicting children in sexually explicit act, etc., in electronic form whereas Section 14 of POCSO Act[7] prescribes Punishment for using child for pornographic purposes.

---

6 ***67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form. -***

Whoever-

(a) *publishes or transmites or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or*

(b) *creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or*

(c) *cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or*

(d) *facilitates abusing children online, or*

(e) *records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,*

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of Section 67, Section 67A and this Section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing drawing, painting representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bona fide heritage or religious purposes.

Explanation. -For the purposes of this Section "children" means a person who has not completed the age of 18 years.

7 ***14. Punishment for using child for pornographic purposes.—***

(1) *Whoever, uses a child or children for pornographic purposes shall be punished with imprisonment of either description which may extend to five years and shall also be liable to fine and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also be liable to fine.*

(2) *If the person using the child for pornographic purposes commits an offence referred to in Section 3, by directly participating in pornographic acts, he shall be punished with imprisonment of either description for a term which shall not be less than ten years but which may extend to imprisonment for life, and shall also be liable to fine.*

(3) *If the person using the child for pornographic purposes commits an offence referred to in Section 5, by directly participating in pornographic acts, he shall be punished with rigorous imprisonment for life and shall also be liable to fine.*

(4) *If the person using the child for pornographic purposes commits an offence referred to in Section 7, by directly participating in pornographic acts, he shall be punished with imprisonment of either description for a term which shall not be less than six years but which may extend to eight years, and shall also be liable to fine.*

(5) *If the person using the child for pornographic purposes commits an offence referred to in Section 9, by directly participating in pornographic acts, he shall be punished with imprisonment of either description for a term which shall not be less than eight years but which may extend to ten years, and shall also be liable to fine.*

During investigation, the accused S. Harish admitted to having viewed pornography during college, and a forensic analysis of his mobile phone confirmed the presence of CSEAM.

Upon completion of the investigation, a charge sheet was filed on 19th September 2023, against the accused for offenses under Section 67B of the IT Act and Section 15(1) of POCSO. The charge sheet was filed for offence under Section 15(1) POCSO Act[8] instead of Section 14(1) of POCSO Act. Section 15 prescribes punishment for punishment for storage of pornographic material in any form involving a child.

The accused filed a Petition (Crl. O.P. No. 37 of 2024) under Section 482 of the Code of Criminal Procedure, 1973, in the High Court of Judicature at Madras, seeking to quash the charge sheet. The High Court of Madras allowed the petition and quashed the chargesheet vide order dated 11th January 2024, effectively terminating the criminal proceedings against the respondent.

Findings of The High Court

- Merely possessing or watching child pornography in private, without publishing or transmitting it, does not constitute an offense under Section 14(1) of the POCSO Act, to make out an offense under this Section, there must be evidence that the accused used a child for pornographic purposes.

It is apparent that the observation Hon'ble HC revolved around Section 14 of POCSO Act and reaffirming that in Order to apply Section 14(1) of the POCSO Act there must be explicit publication or transmission of child pornography.

- Section 67B of the IT Act only makes the act of transmission, publication or creation of material depicting children in a sexually explicit manner an offence. Mere watching or downloading of child pornography in private domain is not punishable under the same.

8 **15. Punishment for storage of pornographic material involving child.--** *(1) Any person, who stores or possesses pornographic material in **any form** involving a child, but fails to delete or destroy or report the same to the designated authority, as may be prescribed, with an intention to share or transmit child pornography, shall be liable to fine not less than five thousand rupees and in the event of second or subsequent offence, with fine which shall not be less than ten thousand rupees.*

(2) Any person, who stores or possesses pornographic material in any form involving a child for transmitting or propagating or displaying or distributing in any manner at any time except for the purpose of reporting, as may be prescribed, or for use as evidence in court, shall be punished with imprisonment of either description which may extend to three years, or with fine, or with both.

(3) Any person, who stores or possesses pornographic material in any form involving a child for commercial purpose shall be punished on the first conviction with imprisonment of either description which shall not be less than three years which may extend to five years, or with fine, or with both and in the event of second or subsequent conviction, with imprisonment of either description which shall not be less than five years which may extend to seven years and shall also be liable to fine.

Hon'ble HC, apparently observed that, in lines where is similar to Section 14(1) of the POCSO Act, in order to constitute an offence under 67B there must be overt act of transmission, publication, creation of child pornography material which was missing in this case.

The appellants, a group of NGOs working against child trafficking and sexual exploitation, appealed to the Supreme Court, challenging the High Court's ruling.

Issues before the Supreme Court

1. Scope of Section 15 of the POCSO Act.
2. True scope of Section 67B of the IT Act.
3. Whether the viewing of child pornographic material is punishable under Section 15 of the POCSO Act and Section 67B of the IT Act?
4. Foundational facts necessary for invoking the statutory presumption of culpable mental state i.e. Section 30 of POCSO Act[9] in respect of Section 15 of the POCSO Act.
5. Can the statutory presumption of a culpable mental state under Section 30 of the POCSO Act be invoked during quashing proceedings under Section 482 of Cr.P.C.?

Decision

The Hon'ble Supreme Court, in a judgment, overturned the decision of the High Court and restored the criminal proceedings against the respondent. The Court found that the High Court had committed an egregious error by quashing the criminal proceedings without even properly perusing the chargesheet and other material on record and consequently set aside the impugned judgment and order. The Court examined the legal provisions under the POCSO Act and the IT Act and elaborated on the scope of these statutes, particularly regarding the possession, consumption, and transmission of CSEAM.

9 Section 30. Presumption of culpable mental state.
(1) In any prosecution for any offence under this Act which requires a culpable mental state on the part of the accused, the Special Court shall presume the existence of such mental state but it shall be a defence for the accused to prove the fact that he had no such mental state with respect to the act charged as an offence in that prosecution. Cont…(2) For the purposes of this Section, a fact is said to be proved only when the Special Court believes it to exist beyond reasonable doubt and not merely when its existence is established by a preponderance of probability. *Explanation*.--In this Section, "culpable mental state" includes intention, motive, knowledge of a fact and the belief in, or reason to believe, a fact.

Findings

Scope of Section 15 of the POCSO Act

- **The Concept of Inchoate Offence under Section 15 of the POCSO Act**

The Court recognized that the consumption of CSEAM, coupled with the failure to delete or report it, constitutes an offense under the POCSO Act, as it is an "Inchoate Crime" or "Inchoate Offense"—an offense committed in preparation for a further crime.

- **Three Distinct Offenses under Section 15:**

Section 15(1): Storing/possessing child pornography without deleting/destroying/reporting, with intent to share/transmit. The use of the words *"with an intention to share or transmit child pornography"* in the said provision makes it clear that ***no actual sharing or transmission is required to constitute the offence and mere possession shall be sufficient cause for the offence.***

Section 15(2): Storing/possessing for transmitting, displaying, propagating, or distributing. The use of the words *"for transmitting or propagating or displaying or distributing in any manner at any time"* clearly suggests that again no actual act of transmission, propagation, display or distribution is required to take place.

Section 15(3): Storing/possessing for commercial purposes. To constitute an offence under this provision, the requirement is that the storage or possession of any child pornography must be in lieu of any monetary gain or for receiving any other valuable consideration irrespective of whether such monetary gain or valuable consideration is actually generated or acquired. Therefore, if the purpose of storing or possessing child pornographic material is for commercial gain, it itself is an offence and it cannot be a defence that there was no actual monetary gain or valuable consideration.

Viewing is equivalent to possession

- The Supreme Court clarified that viewing CSEAM is equivalent to possession under Section 15(1) of the POCSO Act. This is a shift from the pre-2019 framework, where Section 15 only criminalized storage of CSEAM for commercial purposes. The 2019 Amendment to the POCSO Act expanded the scope to include possession of CSEAM as a criminal act. The Court acknowledged that possession can be "constructive possession," meaning the person may not physically possess the material but has control over it through devices or

other means. Even if the material is deleted, if a person exercises control over it, such as viewing it, it amounts to possession.

- Even if evidence is found that CSEAM was stored or possessed at any point of time, the offense would apply, regardless of when the criminal proceedings were initiated. In this connection Hon'ble Apex Court has observed that Section 15 of the POCSO Act does not specify that the possession or storage of CSEAM must be contemporaneous with the filing of the FIR

Concept of 'Possession', 'Constructive Possession', and 'Immediate Control' under Section 15 of the POCSO Act and in reference of Child Pornographic Issue:

The Hon'ble Apex Court has also elaborated upon Concept of 'Possession', 'Constructive Possession', and 'Immediate Control' under Section 15 of the POCSO Act. Hon'ble Apex Court observed that in cases of possession of child pornography under Section 15 of the POCSO Act, when a person views child pornography online, but does not download it onto their device, they might not have physical custody over the material. However, their control over the material can still be considered possession. Possession implies the ability to exercise control over the material, including actions like viewing, manipulating (e.g., zooming in), or distributing the material. Thus, the law holds individuals accountable not just for storing or saving such material but also for accessing and controlling it, even temporarily, through the use of a device. For such cases the Hon'ble Apex Court applied the principle of constructive possession. For example, a person may not have physically stored the child pornography on their device but could access it at any given time, or possess the ability to share, delete, or alter it. The law recognizes that constructive possession is equivalent to physical possession because the individual maintains the authority to control the material.

In addition to possession and constructive possession, **immediate control** refers to a situation where a person has direct control over the material, even if the possession is temporary. Immediate control is typically evident in cases where an individual can access, view, or manipulate the material at that moment but may not necessarily store it for an extended period. This form of control implies that the person can decide what to do with the material, such as viewing, saving, forwarding, or deleting it.

For example, an individual might receive a link leading to child pornography via text or social media and, upon clicking it, the material opens on their device. Even if they haven't stored the material on their device, they still exercise immediate control over it at that moment because they have the ability to decide what happens next, such as whether they want to keep or delete the content.

The Hon'ble Apex Court differentiated the situation when a person might possess CSEAM but without knowledge. In this connection Hon'ble Apex Court observed that without knowledge, an individual cannot be deemed to have possessed or controlled the material, as they would not have been in a position to exercise control over it effectively.

Scope of Section 67B of the IT Act

Section 67B of the IT Act criminalizes the creation, possession, propagation, consumption, and dissemination of CSEAM. The Court held that the provision covers both direct and indirect acts of online sexual exploitation and abuse of children, making it applicable not only to dissemination but also to the mere possession or consumption of such material.

Analysis of Section 67B

- Section 67B(a): Dissemination of Child Pornography
    - Penalizes publication or transmission of material involving a child in sexually explicit acts.
    - Requires actual publication/transmission and involvement of the accused in the process.
- Section 67B(b): Creation, Collection, and Engagement with Child Pornographic Material
    - Covers creation of text or image-based content depicting children in obscene/ indecent/sexually explicit manner.
    - Penalizes collection, browsing, downloading, advertising, promotion, exchange, or distribution of such material.
    - More expansive than 67B(a), including creation and engagement with material.
- Section 67B(c): Enticement of Children for Sexual Acts
    - Penalizes inducing or enticing a child to participate in sexually explicit acts using computer resources.
    - Actual inducement/enticement is sufficient; child's participation not necessary for offense.
- Section 67B(d): Facilitation of Online Child Abuse
    - Penalizes any form of facilitation of online child abuse.

- No specific intention required; act must have the likelihood to aid or enable online child abuse.

- Section 67B(e): Recording of Sexual Acts Involving Children
  - Penalizes recording of sexually explicit acts with or in the presence of a child.
  - Child need not be physically present; exposure to such acts (e.g., through video) is sufficient.

Section 30 of POCSO: Presumption of Culpable Mental State

- Special Court *shall* presume existence of culpable mental state in prosecutions under POCSO;
- Accused may rebut this presumption by proving lack of such mental state;
- Standard of proof for rebuttal by accused: beyond reasonable doubt.

In order to invoke statutory presumption of Section 30 of POCSO Act, the prosecution must establish foundational facts. The Hon'ble Apex Court has also led down for the purpose of Section 15 of POCSO Act as to what would constitute foundational facts:

(a) For Section 15(1)- the necessary foundational facts would be to establish the storage or possession of any child pornographic material and that the person accused had failed to delete, destroy or report the same.

(b) For Section 15(2) the prosecution would be required to first establish the storage or possession of any child pornographic material, and also any other fact to indicate either the actual transmission, propagation, display or distribution of any such material or any form of an overt act such as preparation or setup done for the facilitation of the transmission, propagation, display or distribution of such material, whereafter it shall be presumed by the court that the said act was done with the intent of transmitting, displaying, propagating or distributing such material and that the said act(s) had not been done for the purpose of either reporting or for use as evidence.

(c) For Section 15 (3) the prosecution must establish the storage or possession of such material and further prove any fact that might indicate that the same had been done to derive some form of gain or benefit or the expectation of some gain or benefit.

The Supreme Court ruled that Section 30 of the POCSO Act creates a rebuttable presumption of a culpable mental state when the offense requires malicious intent. This presumption can assist the prosecution, as it is often difficult to establish direct evidence of malicious intent in cases

involving inchoate crimes. The Court ruled that when High Courts deal with quashing petitions, they can rely on this statutory presumption to avoid bypassing the legislative presumption concerning malicious intent. However, the presumption may be disregarded if no foundational facts have been established by the prosecution.

Suggestions to the Union Government

1. The Court recommended that the term "child pornography" be replaced with "child sexual exploitation and abuse material" (CSEAM) to more accurately reflect the criminal nature of the offense and highlight the harm caused to children.
2. Amend Section 15 of the POCSO Act to make it easier for the public to report CSEAM via an online portal.
3. Conduct public awareness campaigns about the realities of CSEAM and its consequences to help reduce its prevalence.
4. Courts should use the term "child sexual exploitation and abuse material" (CSEAM) instead of "child pornography" in all judicial orders and judgments.
5. Provide support services for victims and rehabilitation programs for offenders, including psychological counseling, therapeutic interventions, and educational support.
6. Implement comprehensive sex education programs that include information about the legal and ethical ramifications of CSEAM to help deter potential offenders, as well as raising awareness about POCSO among children from an early age and consider constituting an Expert Committee to devise this comprehensive program.
7. Implement early identification and intervention strategies for youth with problematic sexual behaviors (PSB), including training for educators, healthcare professionals and law enforcement to recognize warning signs and to educate students about healthy relationships, consent, and appropriate behavior to help prevent PSB.

ILLUSTRATIONS

In the context of storage possession and downloading the Hon'ble Apex Court has also mentioned illustrative situations which would constitute offence under section 15 of the POCSO act.

A. CSEAM found in working mobile:

The discovery of child pornographic material stored on 'A's personal mobile phone, which was neither deleted, destroyed, nor reported, attracts a violation of Section 15(1) of the POCSO Act. While there is no evidence of active transmission, display, or distribution of the material, the failure to take action implies an intent to share or transmit it. This omission strongly indicates a deliberate intent, making it likely that the failure to delete or report the material was to facilitate its spread, thus constituting an offence under Section 15(1) of the POCSO Act.

B. CSEAM found in a broken phone

Child pornographic material was found stored on a broken mobile phone of 'A', which had never been deleted, destroyed, or reported. While there is no evidence of transmission, propagation, display, or distribution, the material's storage is only violative of Section 15(1) of the POCSO Act and not of Section 15 (2) of the POCSO Act. The broken state of the phone likely prevented 'A' from taking action to delete, destroy, or report the material, rather than showing a deliberate intent to facilitate its spread. As such, the omission does not indicate an intent to share or transmit, and no offence would be constituted under Section 15(1) of the POCSO Act.

C. The case of automatic download:

Child pornographic material was found on 'A's mobile phone due to an automatic download, which 'A' was unaware of. Although the material was stored on the phone, 'A' did not delete, destroy, or report it due to lack of knowledge about the existence of such material on his parts. Since there was no intent to share or transmit the material, the omission is not enough to constitute an offence under Section 15(1) of the POCSO Act.

D. CSEAM along with chats

(i) Child pornographic material was found on 'A's mobile phone, and there were also chats where 'A' told his friend 'B' that he had the material and could share it. This shows that 'A' took steps to distribute the material, making him liable under Section 15(2) of the POCSO Act.

(ii) Child pornographic material was found on 'A's mobile phone, and he created a chat group with several friends, where he stated that he had the material and would share it in the group. This shows that 'A' took direct actions to distribute the material, making him liable under Section 15(2) of the POCSO Act.

(iv) Child pornographic material was found stored in several television devices in a hotel run by 'A'. Since the material was stored on multiple devices in a public space, it suggests that 'A' was using the hotel and its televisions to display the child pornographic material. Therefore, 'A' would be punishable under Section 15(2) of the POCSO Act.

E. CSEAM material for commercial gain:

(i) 'A' has child pornographic material on his phone and creates a group with several friends, offering to send the material in exchange for money. Since 'A' is attempting to distribute the material for monetary gain, this shows he took steps for financial profit, making him liable under Section 15(3) of the POCSO Act.

(ii) Child pornographic material was found stored on several television devices in a hotel run by 'A', and the material had a price listed on it. Since the material was stored in a publicly accessible place and was being offered for money, it indicates that 'A' was using the hotel and televisions to display the material for monetary gain. Therefore, 'A' would be punishable under Section 15(3) of the POCSO Act.

F. Constructive Possession:

'A' regularly views child pornography but does not download it to their computer. Instead, 'A' accesses the material on a streaming website and deletes it after viewing. Even though 'A' doesn't store the material, the court may consider 'A' in constructive possession of the material because they have control over it while viewing, with the ability to alter, manipulate, or delete the content. This concept ensures that an individual cannot evade liability by simply not downloading the material or storing it on their device.

G. Immediate Control:

If 'A' receives a link from 'B' containing child pornography and opens it, 'A' has immediate control over the material at that time. Even though 'A' did not store the material, the act of viewing it and having the option to save, share, or delete it demonstrates immediate control. If 'A' views the material for a considerable amount of time and exercises control over it (e.g., by forwarding it or enlarging it), they would be deemed to be in possession of the material, even though they didn't store it on their device.

Conversely, if 'A' closes the link immediately upon realizing its content, they may not be in possession as they have not exercised sufficient control over it but 'A' will only be absolved of any liability if he after closing the link further reports the same to the authorities. Thus, when it comes to constructive possession of an accused, it is the failure or omission to report that constitutes the requisite actus-reus for the purposes of Section 15 sub Section (1) of POCSO.

H. Possession of CSEAM with(out) knowledge:

If 'A' receives an unknown link from 'B,' and upon clicking it, a child pornographic video opens on 'A's device, 'A' may not initially have knowledge of the material. Since 'A' was unaware of what the link contained at the time of clicking it, they cannot be said to have possessed the material. However, if 'A' continues to view the material and makes decisions to alter, forward, or delete it, 'A' would then have sufficient knowledge to be considered in possession of it, as they now have control over it.

Note: subtitles added for easy understanding of readers

CONCLUSION

The Supreme Court's verdict in Just Right for Children Alliance v. S. Harish has notably strengthened child protection laws in India by categorizing the possession or storage of child sexual exploitation and abuse material (CSEAM) as a criminal offense. This judgement sends a strong deterrent message to potential offenders and has prompted law enforcement to take more proactive measures. It has also increased public awareness, fostering stronger efforts to curb the creation and distribution of such harmful content. Furthermore, the Court introduced the concept of constructive possession, expanding the scope for prosecution to include individuals who, while not physically storing CSEAM, may have control over it through digital devices or other means.

In addition, the Court clarified the responsibility of online intermediaries, ruling that they cannot claim immunity under Section 79 of the IT Act[10] unless they remove CSEAM and notify

10 ***79. Exemption from liability of intermediary in certain cases.***--*(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-Sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.*
(2) The provisions of sub-Section (1) shall apply if--
(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
(b) the intermediary does not--
(i) initiate the transmission,
(ii) select the receiver of the transmission, and

the authorities in accordance with the POCSO Act. Rule 11 of the Protection of Children from Sexual Offences (POCSO) Rules, 2020 requires intermediaries, like social media platforms, to report child abuse and exploitation cases and provide necessary materials to the police or cyber-crime portal. According to an agreement between the National Crime Records Bureau (NCRB) and the National Centre for Missing & Exploited Children (NCMEC), social media platforms must report such cases to NCMEC, which then shares them with NCRB and local authorities in India. However, apex court has also observed that some social media intermediaries only follow this agreement and fail to report directly to local authorities as required by POCSO. The court emphasizes that intermediaries cannot avoid liability under Section 79 of the IT Act unless they follow the mandatory provisions of the POCSO Act, which includes removing child pornography and promptly reporting such content to the relevant police units.

1.3 VARIOUS OTHER FORMS OF CYBER OFFENCES

Although the cyber offences explicitly identified under the Information Technology Act, 2000, as amended in 2008, have been outlined herein. This section covers key offences such as identity theft, impersonation, violation of privacy, and cyber terrorism, along with their corresponding legal provisions and penalties. However, there are several other offences related to cyber-crime which have not been explicitly outlined in the IT Act, 2000. Some other forms of commonly known cyber offences are dealt here in after.

1.3.1 CYBER STALKING

Although there is no defined term but cyber stalking is a form of harassment that extends traditional stalking into the digital realm, using the internet, email, chat rooms, and other online platforms to threaten, harass, or track an individual. It is often a series of actions, each of which might be legal on its own but collectively forms a pattern of harassment. While the definition of cyber stalking may vary across regions, it is generally understood as an ongoing process of intimidation and harm facilitated by technology.

(iii) select or modify the information contained in the transmission;
(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may pre(3) The provisions of sub-Section (1) shall not apply if--
(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;
(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.
Explanation. -- For the purposes of this Section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.]

Stalking through Computer	In this form of stalking the offender can take control of the computer of the victim as soon as the computer starts operating. This form of cyber stalking requires a high degree of computer knowledge to get access to the target's computer and the remedy available to the victim is to disconnect the computer and abandon the current internet address.
Stalking through the Internet	This is a global form of cyber stalking. In this the offender doesn't invade the private space of the victim but harasses her through the global medium publically. The offender, through the internet medium posts the phone numbers and email address of the victim on porn sites and puts morphed photos of the victim on cyber space and threatens them. This is the serious nature of cyber stalking where the stalker chases all the activity of the victim on the net and posts false information about her on the websites.

Legal Provisions with respect to Cyber Stalking in India

The IT Act, 2008 does not directly address stalking. ***Section 354D in the Indian Penal Code, 1860*** (which is now ***Section 78 in the Bharatiya Nyaya Sanhita, 2023***) to define and punish the act of stalking.[11]

11 Section 354D, IPC:
(1) Whoever follows a person and contacts, or attempts to contact such person to foster personal interaction repeatedly, despite a clear indication of disinterest by such person, or whoever monitors the use by a person of the Internet, email or any other form of electronic communication, or watches or spies on a person in a manner that results in a fear of violence or serious alarm or distress in the mind of such person, or interferes with the mental peace of such person, commits the offence of stalking:
Provided that the course of conduct will not amount to stalking if the person who pursued it shows-
(i) that it was pursued for the purpose of preventing or detecting crime, and the person accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the state; or
(ii) that it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or
(iii) that in the particular circumstances the pursuit of the course of conduct was reasonable.
(2) Whoever commits the offence of stalking shall be punished with imprisonment of either description for a term which shall not be less than 1 year but which may extend to 3 years, and shall also be liable to fine.

1.3.2 VIRUS

Computer viruses are as common as the common cold. Just as some dust and insects are likely to creep into the home despite several precautions are taken similarly computer virus get into the computer through a CD, floppy or pen-drive that is corrupted or through the Internet where they where they spread like airborne viruses that cause colds, fevers, or more severe illnesses.

Section 43-(c) of the I.T. Act, 2000 imposes a monetary liability by way of compensation upon a person who, without the permission of the owner or in-charge of a computer, introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network. "Computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

Section 43 imposes a strict liability upon the person who plants any computer virus or contaminant. All the violations stipulated in Section 43 including clause (c) that covers the violation of introduction or causing the introduction of any computer contaminant or computer virus into any computer, have also been made criminal offences. Hence, dishonestly or fraudulently introducing or causing the introduction of a computer virus or computer contaminant into another's computer, would also constitute a criminal offence entailing an imprisonment of three years.

Challenges with the issue of Viruses:

1. Lack of awareness: There is minimal awareness in India about computer viruses, contaminants, and anti-virus software.
2. Limited expertise: Law enforcement agencies lack the necessary expertise to trace the exact source of a virus.
3. Difficulty in tracking sources: Identifying the source of a virus is challenging due to the nature of viruses as it rapidly spreads in the cyberspace..
4. Unawareness of infection: A person may not even be aware that their computer is infected with a virus.
5. Evolving threats: New viruses are constantly being developed, and many of which are undetectable by existing anti-virus software.

6. Unintentional transmission: Even with anti-virus software, viruses can still sneak in and unknowingly be transmitted to others.

7. Potential for false allegations: Without clear intent (mens rea), there is a risk of false accusations and baseless criminal cases regarding virus planting.

8. Prolonged legal struggles: Individuals accused of virus-related crimes may face a lengthy legal process, only proving their innocence at the defense stage.

1.3.3 CYBERCRIME RELATED TO FINANCE

Cybercrime in the financial sector refers to criminal activities aimed at gaining illicit financial profit, such as identity theft, ransomware attacks, online fraud, and attempts to steal payment card or financial account details. Essentially, it involves crimes like stealing credit card information, accessing bank accounts to carry out unauthorized transactions, using stolen identities to apply for financial products, and more. The financial industry is a prime target for such cybercriminals due to its high value, but these crimes also affect businesses and individuals alike. Anyone can fall victim to scams like credit card skimming, hacking of digital wallets, or malware designed to capture passwords.

TYPES	DEFINITION	How do fraudsters operate?	How to protect yourself from fraud:
SIM Swap	Under SIM Swap, fraudsters manage to get a new SIM card issued against your registered mobile number through the mobile service provider. With the help of this new SIM card, they get One Time Password (OTP) and alerts, required for making financial transactions through your bank account. Under SIM Swap, fraudsters manage to get a new SIM card issued against your registered mobile number through the mobile service provider. With the help of this new SIM card, they get One Time Password (OTP) and alerts, required for making financial transactions through your bank account.	Step – 1 :: Fraudsters gather customer's personal information through Phishing, Vishing, Smishing or any other means. Step – 2:: They then approach the mobile operator and get the SIM blocked. After this, they visit the mobile operator's retail outlet with the fake ID proof posing as the customer. Step – 3:: The mobile operator deactivates the genuine SIM card and issues a new one to the fraudster. Step – 4:: Fraudster then generates One Time Password (OTP) required to facilitate transactions using the stolen banking information. This OTP is received on the new SIM held by the fraudster.	• If your mobile no. has stopped working for a longer than usual period, enquire with your mobile operator to make sure you haven't fallen victim to the Scam. • Register for SMS and Email Alerts to stay informed about the activities in your bank account. • Regularly check your bank statements and transaction history for any irregularities.

Vishing	Vishing is one such attempt where fraudsters try to seek your personal information like Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.	Step – 1 The fraudster poses as an employee from the bank or a Government / Financial institution and asks customers for their personal information. Step – 2 They cite varied reasons as to why they need this information. For e.g. reactivation of account, encashment of reward points, sending a new card, linking the Account with Aadhar, etc. Step – 3 These details thus obtained are then used to conduct fraudulent activities/ transactions on the customer's account without their knowledge.	• Never share any personal information like Customer ID, ATM PIN, OTP etc. over the phone, SMS or email. • If in doubt, call on the Phone Banking number of your Bank.

Smishing	Smishing is a type of fraud that uses mobile phone text messages to lure victims into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web.	Step – 1 Fraudsters send SMS intimating customers of prize money, lottery, job offers etc. and requesting them to share their Card or Account credentials. Step – 2 Unaware, the customer's follow instructions to visit a website, call a phone number or download malicious content. Step – 3 Details thus shared with the person who initiated the SMS are then used to conduct fraudulent transactions on the customer's account, causing them financial loss.	• Never share your personal information or financial information via SMS, call or email. • Do not follow the instructions as mentioned in SMS sent from un-trusted source, delete such SMS instantly.

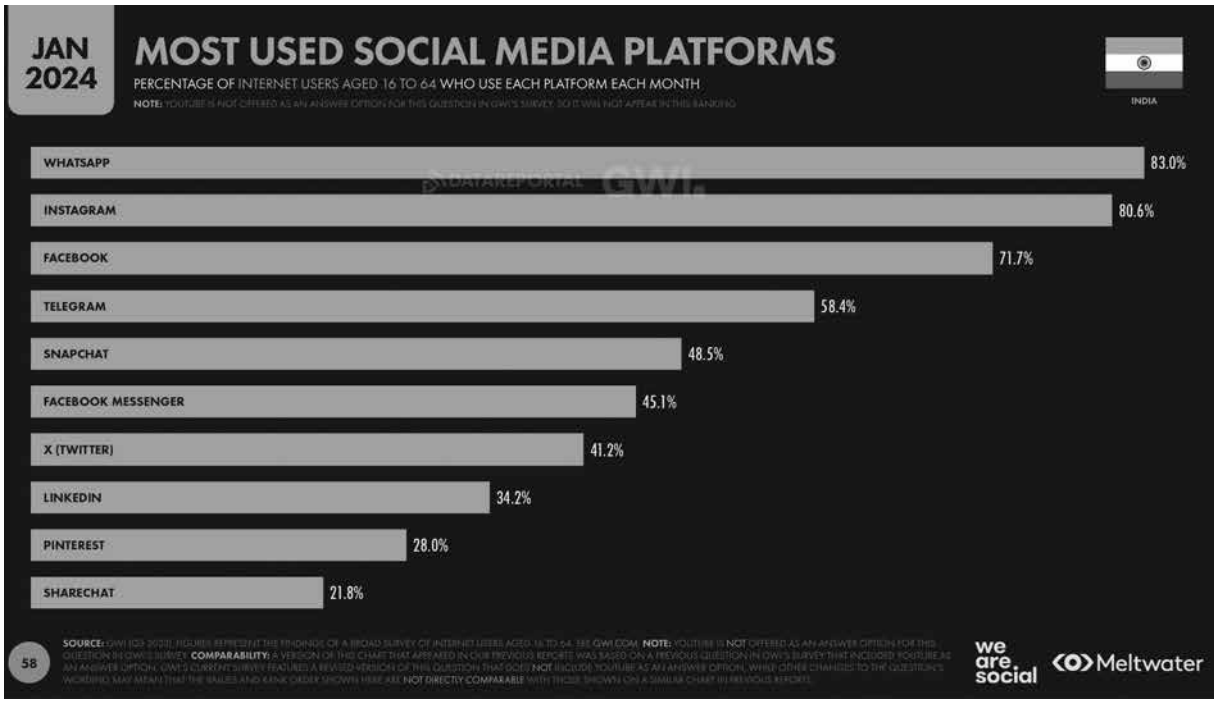
Phishing	Phishing is a type of fraud that involves stealing personal information such as Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc. through emails that appear to be from a legitimate source. Nowadays, phishers also use phone (voice phishing) and SMS (Smishing). To understand the process to verify website readers may refer to the link*	Fraudsters pose as Bank officials and send fake emails to customers, asking them to urgently verify or update their account information by clicking on a link in the email. Clicking on the link diverts the customer to a fake website that looks like the official Bank website – with a web form to fill in his/her personal information. Information so acquired is then used to conduct fraudulent transactions on the customer's account.	• Always check the web address carefully. • always type the website address in web browser address bar. • Install the latest anti-virus/anti spyware/ firewall/security patches on your computer or mobile phones. • DO NOT click on any suspicious link in your email. • DO NOT provide any confidential information via email. • DO NOT open unexpected email attachments or instant message download links. • DO NOT access Net Banking or make payments using your Credit / Debit Card from computers in public places like cyber cafés or even from unprotected mobile phones.

* - chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.jogulambagadwalpolice.telangana.gov.in/PDF/TYPES-OF-CYBER-CRIMES.pdf

Money Mule	Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen/illegal money via their bank account(s). When such incidents are reported, the money mule becomes the target of police investigations, due to their involvement.	Step – 1 Fraudsters contact customers via emails, chat rooms, job websites or blogs, and convince them to receive money into their bank accounts, in exchange for attractive commissions. Step – 2 The fraudsters then transfer the illegal money into the money mule‘s account. Step – 3 The money mule is then directed to transfer the money to another money mule‘s account – starting a chain that ultimately results in the money getting transferred to the fraudster‘s account. Step – 4 When such frauds are reported, the money mule becomes the target of police investigations. How to protect yourself from fraud: Do not respond to emails asking for your bank account details.	• Do not respond to emails asking for your bank account details. • For any overseas job offer, first confirm the identity and contact details of the employing company. • Do not get carried away by attractive offers/ commissions or consent to receive unauthorized money.

Trojan	A Trojan is a harmful piece of software that users are typically tricked into loading and executing on their computers. After it is installed and activated, Trojan attacks the computer leading to deletion of files, data theft, or activation/spread of viruses. Trojans can also create back doors to give access to hackers.	Step – 1 Fraudsters use spamming techniques to send e-mails to numerous unsuspecting people. Step – 2 Customers who open or download the attachment in these emails get their computers infected. Step -3 When the customer performs account/card related transactions, the Trojan steals personal information and sends them to fraudsters. Step – 4 These details will then be used to conduct fraudulent transactions on the customer's account.	• Never open e-mails or download attachments from unknown senders. Simply delete such emails. • Installing antivirus helps. It scans every file you download and protects you from malicious files. • Enable automatic OS updates or download OS patch updates regularly to keep your Operating System patched against known vulnerabilities. • Install patches from software manufacturers as soon as they are distributed. A fully patched computer behind a firewall is the best defense against Trojan. • Download and use the latest version of your browser. • If your computer gets infected with a Trojan, disconnect your Internet connection and remove the files in question with an antivirus program or by reinstalling your operating system. If necessary, get your computer serviced.

1.3.4 CYBER CRIME RELATED TO SOCIAL MEDIA



So many people are using social networking websites and people feel happy to share about themselves by uploading new videos and photos or by writing some text or comment. However, most of the people are not aware of the drawback of using these sites in access. As the graph shows that India is having big chunk of population who are available on one form or other. The information of that person can be hacked by any person and that information can be misused by other people.

There are a range of activities on the internet which, strictu sensu may not fall inti the category of any offence or crime in general. However at times those activities are very offending and depending upon the intensity andgravity as well as facts and circumstances may be amenable under penal laws of india. The list cannot be exhaustive and some commonly known such activity are listed below.

Below are the common offence being committed on or as a result of Social Media:-

(i) Cyber bullying & Trolling:

The activities like cyber bullying and trolling are not recognised as a crime under statute but depending upon the circumstances either the it act or bns may be applicable to these activities

it is most commonly reported that on social media people bully, harass and troll. If anyone feel threatened by a statement made online about oneself, or believe that the threat is credible, one may pursue legal recourse.

(ii) Buying Illegal Things:

Connecting over social media to make business connections, or to buy legal goods or services may be perfectly legitimate. However, connecting over social media to buy drugs, or other regulated, controlled or banned products is probably illegal.

(iii) Vacation Robberies:

One common practice among burglars is to use social media to discover when a potential victim is on vacation. If vacation status updates are publicly viewable, rather than restricted to friend groups, then potential burglars can easily see when you are going to be away for an extended period of time.

(iv) Creation of fake profile:

Creation of fake profile of a person and posting offensive content including morphed photographs on the fake profile.

(v) Fake online friendship:

Developing online friendship over social media with no real-life familiarity and using the emotional connect may harm into transferring funds on some pretext such as medical emergency, legal troubles, problems in a foreign country etc.

(vi) Image and Video Morphing:

Morphing is a very specific form of digital sexual violence involving transmogrifying or splicing photos or videos, and uploading them, including on pornographic websites. The digital morphing of an image, as a way of attacking women, is a relatively new form of gendered violence. Its prominence has increased as Artificial Intelligence (AI) capabilities have become more sophisticated and easily available to the general public.

(vii) Deep Fake:

Deepfake technology is a type of artificial intelligence used to create convincing fake images, videos and audio recordings. The term describes both the technology and the resulting bogus content and is a portmanteau of deep learning and fake.

Deepfakes often transform existing source content where one person is swapped for another. They also create entirely original content where someone is represented doing or saying something they didn't do or say.

The greatest danger posed by deepfakes is their ability to spread false information that appears to come from trusted sources. While deep fakes pose serious threats, they also have legitimate uses, such as video game audio and entertainment, and customer support and caller response applications, such as call forwarding and receptionist services.

Difference between morphing and deepfake

Deepfake, put simply, is a method of digitally altering an image, video, audio or other forms of media. But, so is morphing. The difference comes in the algorithms used for the transformation and the purpose of such an act. Deepfakes use deep learning, in which a computer is trained with a heavy amount of data to do human-like tasks. That is where the 'deep' in the name comes from. The 'fake' part of it, refers to the artificially generated output, much like a human-generated one.

Deepfakes are usually created by training a neural network with a large number of images or videos of a specific person. The system learns how to replicate the person's facial movements, expressions, and voice, which can then be superimposed onto another person's performance to create convincingly realistic fabrications.

Morphing, on the other hand, does not rely on AI. It is often used in movies, music videos, and other forms of entertainment to create a transformation effect. Morphing uses a straightforward technique, blending two images to create another image with simple software. For creating deepfake, the technology used is more sophisticated and produces content with a high degree of realism.

1.3.5 DENIAL OF SERVICE ATTACK

A Denial-of-Service (DoS) attack is a type of cyber assault where the attacker floods the target's network or email inbox with a large amount of traffic or spam, disrupting access to crucial services. The server, unable to identify the user, waits for a response and eventually terminates the connection. Meanwhile, the attacker continues sending new forged requests, keeping the server occupied and blocking legitimate users from accessing the services indefinitely.

1.3.6 DATA THEFT

Data and information are valuable assets in this digital age. Business secrets, technical knowhow, designs, music, films, books, personal data including usernames, credit card numbers and

passwords, are some forms of property that drive the information economy. Money, time, effort and creativity go into the creation and compilation of data and information. Stealing of data and information through hacking and other means, is the most prevalent cyber crime.

Data/information theft can be said to be committed in six ways, in other words, it has the following species:

- The first unauthorized copying of data / information;
- Making unauthorized subsequent copies;
- Making a copy and dishonestly sending the data/information online;
- Unauthorized copying of data / information in a floppy, C.D. or pendrive and dishonestly taking it away;
- Stealing the computer itself;
- Data / Information already reside in a movable storage medium (floppy, C.D. or pen-drive) that is dishonestly taken away.

Applying the definition of theft in the Bharatiya Nyay Sanhita, 2023 to the above species, some of the above may be an of 'theft' under section 303.

The I.T. (Amendment) Act, 2008 however brings into existence the offence of 'data theft' (even though not encapsulated in a medium such as CD, computer pen-drive or floppy). The clauses of section 43 read with the new version of section 66 that makes the said clause a penal offence, incorporates the offence of 'data theft' in the true sense of the expression from the legal perspective.

1.3.7 DATA DIDDLING

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating; recording, encoding, examining, checking, converting, or transmitting data. This is one of the simplest methods of committing a computer-related crime, because it requires almost no computer skills whatsoever. Despite the ease of committing the crime, the cost can be considerable.

Data Diddling under Indian Law

In India, alteration of data available in computer resources or diminishing its value or utility or affecting it injuriously so as to cause wrongful loss or damage to the public or any person would be an offence punishable under Section 66 of the IT Act. Such kind of computer crime would also come under offences mentioned under Section 43(d) of the IT Act. If anyone commits an offense of data diddling in India, he is liable to be punished for the offence under Section 43(d) read with Section 66 of the I.T. Act and the punishment for the offence as mentioned under this Act is fine not increasing one Crore Rupees.

1.3.8 SALAMI ATTACKS

A Salami Attack, also known as a Salami Slicing Attack, is a fraudulent method where a cyber criminal commits a series of minor, inconspicuous actions or thefts that, when combined, can lead to significant harm or a considerable compromise of data, resources, or assets.These attacks are insidious because they are typically carried out in a way that each individual action remains inconspicuous, making it challenging for security systems to detect a breach until significant damage has already occurred.

Characteristics

- **Incremental Nature:** The theft occurs in small increments, making it less likely to raise suspicion.
- **Automation:** Often, these attacks are automated through scripts or programs to ensure consistency and scale.
- **Targets:** Common targets include financial institutions, payroll systems, and online subscription platforms.
- **Stealth:** The goal is to avoid detection by ensuring the individual losses are trivial enough to be ignored.

1.3.9 EMAIL BOMBING

E-mail bombing is a form of internet abuse where a large volume of emails is sent to a specific address or mail server in an attempt to overload and crash the system. This can be done by sharing the victim's email address with multiple spammers, causing their inbox or mail servers to be flooded.

1.3.10 DIGITAL ARREST

Digital arrest fraud is a new form of cybercrime in India. These cyber crimes have grave concerns and, hence, these must be addressed at the earliest.

Digital arrest refers to an online scam where cybercriminals impersonate law enforcement officials (such as CBI, Police, or ED) and falsely accuse victims of involvement in criminal activities. They use phone calls or video calls to extort money by claiming the victim is under investigation and keeping them under constant surveillance until their demands are met.

Modus Operandi of Digital arrest

Caller ID Spoofing	Scammers disguise their phone number to look like it is from a legitimate government office or police department. Scammers also reach out via video calls using WhatsApp or Skype.
Intimidation	Victims are falsely accused of crimes like drug trafficking or money laundering, and are shown fake documents and setups that mimic police stations. The scammers use fear tactics, such as threatening jail-term or property seizure, to create urgency.
Isolation	Victims are instructed to remain on the call and not to contact anyone else. This creates a sense of urgency and fear. The fraudsters also use deepfake videos and fake arrest warrants to impersonate officials of law enforcement agencies.

Demands for Money and Personal Identity Theft	The fraudsters demand immediate payment, often via gift cards, wire transfers, or cryptocurrency, which would make the money transfer difficult to trace. Some scammers ask for Aadhaar Details, Bank account details, and other personal information, which are later used for identity theft.

Efforts of the Government

- Indian Cyber Crime Coordination Centre (I4C)- The Indian Cyber Crime Coordination Centre (I4C), part of the cyber and information security division of the Union Ministry of Home Affairs, is dedicated to address rising cybercrime. Between January and April 2024, I4C recorded Rs 120.30 crore in losses by Indians due to digital arrest scams.
- Initiatives and Collaborations- I4C, in partnership with Microsoft, has blocked over 1,000 Skype IDs associated with these scams and launched public awareness campaigns.
- Interministerial committee against transnational crime-In May 2024, an inter-ministerial committee, comprising various law enforcement and intelligence agencies, was established to address the increase in transnational cybercrimes targeting Indians, especially from Southeast Asian countries like Cambodia.

Reporting Cybercrime-Individuals targeted by cyber scams can report incidents immediately via the cybercrime helpline at 1930 or online at cybercrime.gov.in and notify local police.

Chapter 2. Investigation of Cyber Offence

2.1 INVESTIGATION OF CYBER OFFENCES

Unlike the manner in which offences have been traditionally committed, in the cases of cyber offence, the offender is not present at the location of commission of offence; hence the chances of offender getting caught are less. It is difficult for law enforcement agencies to follow traditional investigative steps to prosecute the perpetrator owing to the different location and jurisdiction of the perpetrator.

Extra-territorial Jurisdiction under Indian Law

The cyber offences due to its very nature can expand in more than one jurisdiction, therefore, Section 1(5) of BNS[12] (corresponding Section 4) of IPC and Section 75 of IT Act[13] have an important bearing to understand the procedure for registration of FIR as well as for inquiry and trial into such offences. A bare-reading of Section 1(5) of BNS indicate that the *mandate of BNS would expand to any offence committed by any person in any place without and beyond India even if such offence targets a "computer source"[14] located in India*. Whereas, Section 75 of IT Act 2000, which is wider in ambit than Section 1(5) of the Nyaya Sanhita, 2023 also include jurisdiction in cases where offences committed abroad involving a computer, computer system or computer network located in India, and not just where the computer resource targeted is located in India as is the case under BNS.

It is apparent from a bare reading of Section 75 IT Act that Section 75 IT Act is wider in ambit than Section 1 of BNS. However, Section 75 of the IT Act, 2000 have its own limitations. For instance, Section 75 appears to be ineffective on the ground that if an act is an offence or contravention

12 Section 1(5)1 of the Nyaya Sanhita, 2023 (BNS)(corresponding Section 4 IPC) states— The provision of this Sanhita apply also to any offence committed by— (a) any citizen of India in any place without and beyond India; (b) any person on any ship or aircraft registered in India wherever it may be; and (c) any person in any place without and beyond India committing offence targeting a computer resource located in India.

Explanation.—In this section the word "offence" includes every act committed outside India which, if committed in India, would be punishable under this Sanhita.

13 –(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality. (2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India

14 2 (k) "computer resource" means computer, computer system, computer network, data, computer data base or software

under this Act and is committed by a person from outside India and which is affecting any computer or computer system or computer network in India and that act is not an offence in that country, then any judgment passed by an Indian Court may not be enforced by the Court of that foreign country because that foreign court may not accept the principle of extraterritorial jurisdiction as given under Section 75 as that Act in that country is not considered unlawful.[15]

Reporting of Cyber Offences

In a criminal case for cyber offences FIR can be registered under **Section 173 of Bhartiya Nagrik Suraksha Sanhita (BNSS), (formerly Section 154(1) CrPC)**. With the enactment of the BNSS, 2023, there have been some changes to the legal framework established by the CrPC which can have an important bearing with regard to cyber offences and the same is enumerated below:

(i) Zero FIR: The use of phrase in Section 173 (1) *".....irrespective of the area where the offence is committed....."* connotes that the concept of Zero FIR has been given a statutory basis.

(ii) Information by electronic communication : Now the law mandates that there is requirement of the same to be signed within three days.

In cases for investigation into cyber offences, the principle guiding source would be BNSS (erstwhile CrPC), wheresoever applicable, however, the investigation officers must also be conscious of powers conferred under IT Act, manuals, if any, provided by the state police department and guidelines laid down by the Hon'ble High Courts and Supreme Court.

The difficulty to collect information / gather evidence from abroad: The Ministry of Home Affairs, Govt. of India have prescribed guidelines[16], letter of request, MLAT and Letter Rogatory[17], for gathering information outside India. It is pertinent to mention that Section 166- A (Section 112 BNSS) provides for the process for making a request to any foreign country to help and assist in the investigation. Whereas Section 166 – B CrpC (Section 113 BNSS) talks about letter of request from a country outside India to investigate in India. It is important to note that under Section 112 BNSS, the letter of request can be issued by any Criminal Court, but under Section 113 BNSS, the letter of request shall be forwarded to the Chief Judicial Magistrate/ Judicial Magistrate, who will send letter to police for investigation.

15 https://www.scconline.com/blog/post/2024/03/24/jurisdiction-in-cybercrimes-and-civil-disputes/#fn7

16 *https://www.mha.gov.in/sites/default/files/2022-08/ISII_ ComprehensiveGuidelines_17122019%5B1%5D.pdf,* Last accessed on 15.02.2025.

17 Letters rogatory is a formal communication in writing sent by the Court in which action is pending to a foreign court or Judge requesting the testimony of a witness, residing within the jurisdiction of that foreign court, may be formally taken thereon under its direction and transmitted to the issuing court making such request for use in a pending legal contest or action

Provisions supplementing procedure of investigation under IT Act:

It is important to note that as per Section 78 of IT Act, 2000, a Police Officer not below the rank of Inspector shall investigate any offence under the act.

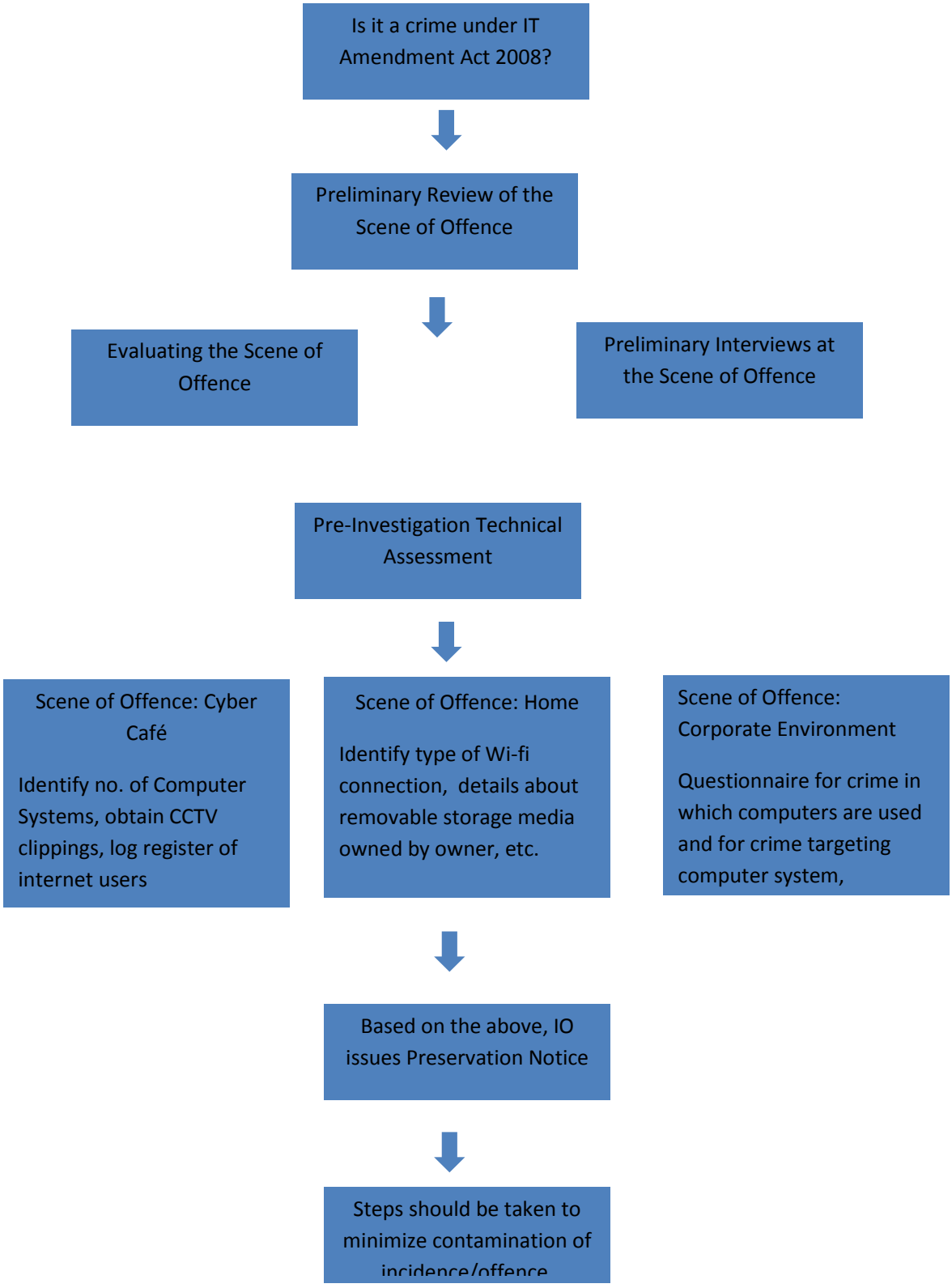
In furtherance to this, as per Section 80 of IT Act, 2000, any police officer, not below the rank of an inspector, may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

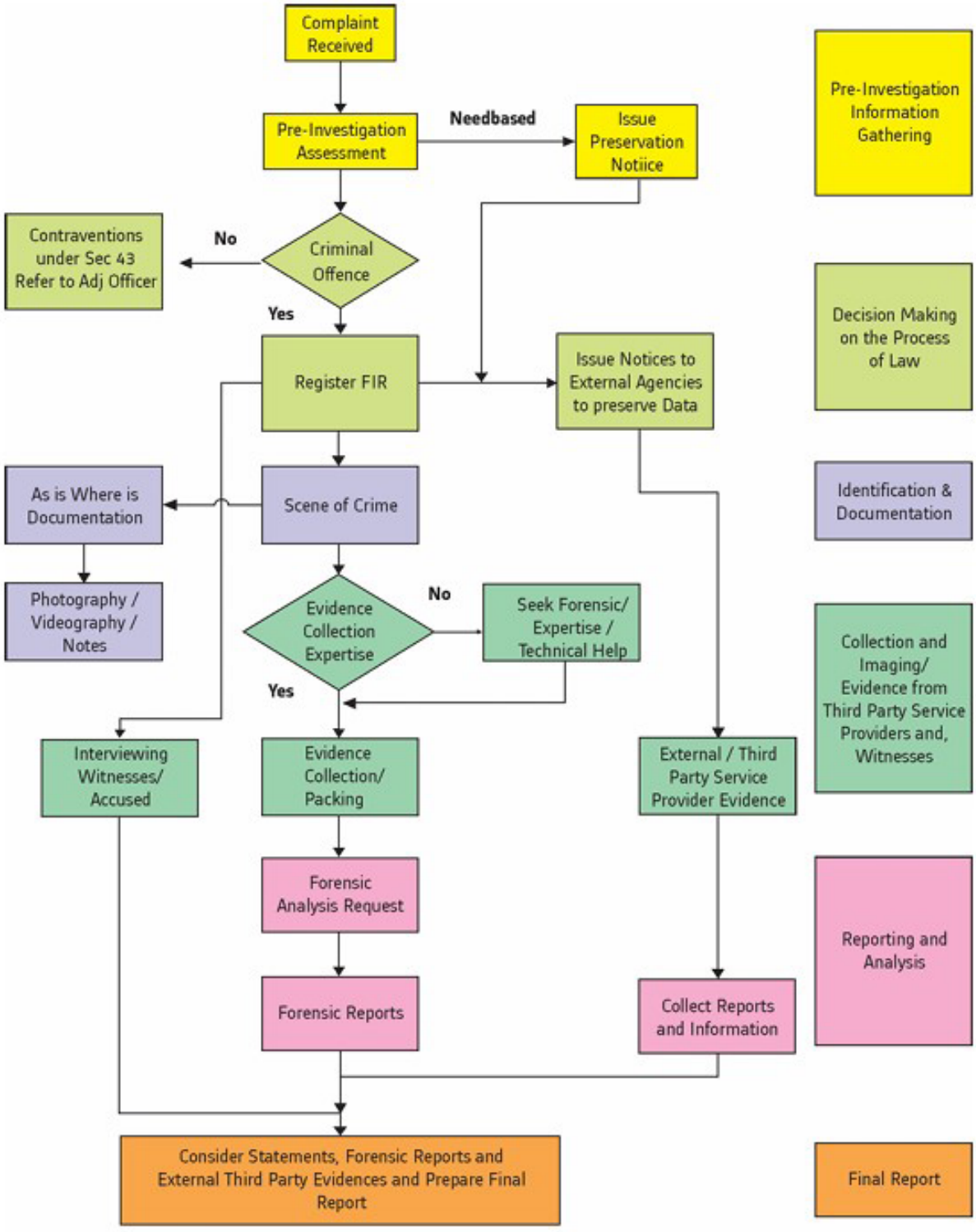
Above two provisions are however, supplementary to the provisions of the CrPC, and both the Acts are applicable unless the provisions of the CrPC are inconsistent with the provisions of the IT Act, in which case the procedure shall be governed by Section 78 and Section 80 of the Act.

Pre – Investigative Assessment[18]

It is a crucial role of an IO to do a pre-investigative assessment for each cyber-crime that is reported. There are few pointers while doing a pre-investigative assessment which are reproduced hereunder:

18 Jharkhand Police: Cyber Crime Investigation Manual, *https://jhpolice.gov.in/downloads/cyber-crime-investigation-manual-dsci-file-size-135-mb-32514-1512041410,* Last accessed on 15.02.2025


Is it a crime under IT Amendment Act 2008?
Preliminary Review of the Scene of Offence
Evaluating the Scene of Offence
Preliminary Interviews at the Scene of Offence
Pre-Investigation Technical Assessment
Scene of Offence: Cyber Café
Identify no. of Computer Systems, obtain CCTV clippings, log register of internet users
Scene of Offence: Home
Identify type of Wi-fi connection, details about removable storage media owned by owner, etc.
Scene of Offence: Corporate Environment
Questionnaire for crime in which computers are used and for crime targeting computer system,
Based on the above, IO issues Preservation Notice
Steps should be taken to minimize contamination of incidence/offence


Complaint Received
Pre-Investigation Assessment
Needbased
Issue Preservation Notiice
Pre-Investigation Information Gathering
Contraventions under Sec 43 Refer to Adj Officer
No
Criminal Offence
Yes
Register FIR
Issue Notices to External Agencies to preserve Data
Decision Making on the Process of Law
As is Where is Documentation
Scene of Crime
Identification & Documentation
Photography / Videography / Notes
Evidence Collection Expertise
No
Seek Forensic/ Expertise / Technical Help
Yes
Collection and Imaging/ Evidence from Third Party Service Providers and, Witnesses
Interviewing Witnesses/ Accused
Evidence Collection/ Packing
External / Third Party Service Provider Evidence
Forensic Analysis Request
Reporting and Analysis
Forensic Reports
Collect Reports and Information
Consider Statements, Forensic Reports and External Third Party Evidences and Prepare Final Report
Final Report

Collection of digital evidence[19]

During an investigation, one of the most crucial step is to collect evidences. As per Jharkhand Police Manual, it stipulates the procedure for gathering evidences from switched – off systems and switched- on systems, as mentioned hereunder:

A) Procedure for gathering evidences from switched – off systems

- Secure and take control of scene of crime both physically (sending all persons away from scene of crime) and electronically (disabling all the network connections.)
- Make sure the computer is switched off, remove the battery from laptop.
- Never switch ON the computers in any circumstances.
- Label and photograph/video of all components of the system.
- Take out storage device (Hard Disk) carefully and record all unique identifiers like model and serial numbers.
- Signature of accused and witness on Hard Disk with a permanent marker.
- After Hard Disk is removed, switch on the system and go to BIOS, also keeping a note of date and time as shown in BIOS.
- Prepare detailed notes giving "when, where, what, why & who" and overall actions taken in relation to the computer equipment.
- Connect the suspected hard drive to the investigator computer through write – block device for forensically previewing/ copying/ printing or for duplication. **NEVER CONNECT DIRECTLY WITHOUT THE BLOCKER DEVICE.**

B) Procedure for gathering evidences from switched – off systems

- Secure the area containing the equipment.
- Move people away from computer and power supply.
- Disconnect the modem if attached.
- If the computer is believed to be networked, seek advice from the technically trained officer, in-house forensic analyst or external specialist.
- Label and photograph/video of all components of the system.

19 *https://jhpolice.gov.in/downloads/cyber-crime-investigation-manual-dsci-file-size-135-mb-32514-1512041410*, last accessed on 15.02.2025

- Remove all other connection cables leading from the computer to other wall or floor sockets or devices.
- Carefully remove the equipment and record the unique identifiers – the main unit, screen, keyboards and other equipment.
- All items must have signed exhibit labels attached to them.
- The equipment should be cooled down before removal.
- Check if there are any passwords, and those must be recorded.
- Detailed notes of all actions taken in relation to computer equipment.
- Keep a note of the content of screen.
- Forensic assistance to be taken for the removal of information present in temporary memory such as RAM.
- If no specialist available then remove the power supply without closing any programs. The power supply cable which is attached at the end of the computer should be removed and not the one attached to the socket.

C) Procedure for gathering evidences from Mobile Phones.

- If the device is "Off", do not turn "ON".
- If device is On, leave ON. Powering down device could enable password, thus preventing access to evidence.
- Photograph device and screen display.
- Keep the device charged.
- Label and collect all cables (including power supply) and transport with device.
- Seize additional storage media
- If device cannot be kept charged, analysis by an expert must be completed prior to battery discharge or data may be lost.
- Document all steps involved in seizure of devices and components.

Current Challenges in Investigations of Cyber Crimes

Since the internet is not tied to a specific area, state or country, there are numerous obstacles in cyber-crime investigation. Cybercrime can be directed from anywhere in the globe and directed at a specific spot.

- **Anonymity and Encryption:** Cyber-attackers manipulate and conceal data using advanced technologies, making it difficult to track them down.
- **Jurisdictional Conflicts:** Cybercrime laws are not uniformly enforced across all countries, complicating prosecution efforts.
- **Lack of Technical Expertise:** Investigators, especially in India, often lack advanced knowledge of digital forensics and cyber investigation techniques. Understanding IP addressing, tracking, and encryption is crucial for tracing perpetrators.
- **Advanced Techniques by Criminals:** Cyber-attackers use sophisticated tools, including AI-driven techniques, to conceal their physical locations and remain undetected.
- **Legal Roadblocks:** Prosecuting cybercriminals from other countries is challenging due to a lack of mutual cooperation. Some governments refuse to sanction prosecutions even when law enforcement identifies the attacker.
- **Absence of a Comprehensive International Legal Framework:** A harmonized legal approach is required to facilitate global cooperation in tackling cybercrime.

2.2 CYBER FORENSICS: SEARCH AND SEIZURE OF ELECTRONIC RECORDS

Unlike traditional evidence such as physical documents or articles, electronic records are more dynamic and susceptible to tampering or loss if not handled properly. The volatile nature of digital data, including data stored in electronic devices, demands that investigators adhere to strict protocols during the search & seizure process. Also, the person investigating the offence has proper training and knows how to deal with electronic devices. The search and seizure of electronic records shall be conducted in accordance with the mandates and provisions of the Code of Criminal Procedure (CrPC) / Bharatiya Nagarik Suraksha Sanhita (BNSS), supplemented by the special provisions of the Information Technology Act, such as Section 78 [20] and section 80[21]. Section 78 grants the authority to investigate offences under the Act exclusively to police officers of the rank of Inspector or above, notwithstanding the provisions of the Code of Criminal Procedure (CrPC). Additionally, Section 80 empowers a police officer of the rank of Inspector or above, or any authorized officer of the Central or State Government, to enter any public place, search, and arrest without a warrant if a person is reasonably suspected of committing, having committed, or being about to commit an offence under the IT Act.

In the case of ***Virendra Khanna v. State of Karnataka,*** **2021 SCC OnLine Kar 5032**,(elaborately dealt later) Hon'ble High Court of Karnataka has also observed that the search and seizure process involves several key stages: identifying relevant devices, securing them to prevent tampering, and meticulously documenting every step. Investigators must note device conditions, connections, and storage media, ensuring all evidence is properly preserved. In the field of investigation into cyber offences cyber forensics has emerged as a critical field. As technology advances, so does the need for effective methods to collect, preserve, and analyze digital evidences. The search and

20 **78. Power to investigate offences**.—Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of [148][Inspector] shall investigate any offence under this Act.

21 **80. Power of police officer and other officers to enter, search, etc.—(**1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a [151][Inspector], or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

Explanation.—For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 (2 of 1974) shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

seizure of electronic records play a pivotal role in ensuring that investigations are conducted in a legally sound and scientifically rigorous manner.

Cyber forensics refers to the application of scientific techniques to collect, preserve, and analyze digital evidence from electronic devices such as computers, smartphones, tablets, servers, and any other digital medium capable of storing or transmitting data. The information stored on these devices can be crucial in proving or disproving criminal activity, from financial fraud to cybercrimes like hacking, identity theft, and data breaches, etc.

As a matter of precaution and to fortify the investigation, investigators should prefer to first obtain legal authorization, typically in the form of a search warrant issued by a court. Section 94 of newly inacted BNSS dealing with the provision in Chapter VII, Summon to produce document or other things falling under the chapter processes to compel the production of things has now explicit provision empowering the court and the investigating officer to order for production of such electronic communication including electronic communication devices which is likely to contain digital evidence. It is also important to mention that such order can also be made either in electronic or physical form.

Since digital evidence is volatile, investigators must take immediate steps to prevent data loss, such as isolating the device from networks or preserving its power state when necessary. Forensic experts play a vital role in data extraction and analysis, using specialized tools to access and recover information without altering its integrity. Forensic examiners then create forensic images bit-by-bit copies of storage media - to prevent alterations to original data. By using advanced forensic tools, forensic examiners analyze extracted information, recover deleted files and track user activity. Finally, a detailed forensic report is prepared and they also document methods of recovering data, and analytical findings to ensure its admissibility in the court. This report must be objective, scientifically valid, and compliant with evidentiary rules, ensuring that the digital evidence can withstand legal scrutiny.

In the case of ***Virendra Khanna v. State of Karnataka*, 2021 SCC OnLine Kar 5032**, the Karnataka High Court has impressed upon that in cases of search of electronic devices in some cases, consent from the device owner may suffice, but searches must remain within legal boundaries to prevent overreach. Also highlighting the importance of preserving integrity of electronic evidence, the Hon'ble High court has emphasized upon maintaining an unbroken chain of custody and requiring thorough documentation from the moment of seizure to forensic analysis.

In this case the Hon'ble Karnataka High Court has addressed several important issues concerning the furnishing of passwords, passcodes, or biometrics by an accused and the associated legal

considerations with electronic devices and records. Here are the key questions answered in the case:[22]

Q1. Can an accused be directed to provide the password, passcode, or biometrics to unlock a smartphone or email account?

Ans. During an investigation, it is common for the Investigating Officer to issue directions or make requests for information, material objects, or other relevant details. As part of this process, the officer may ask the accused to furnish access credentials such as a password, passcode, or biometrics. *However, compliance with such a request remains at the discretion of the accused.* If the accused chooses to provide the requested credentials, the Investigating Officer may use them to access the device or account as part of the investigation.

Q2. What recourse is available to an Investigating Officer if the accused refuses to provide the password, passcode, or biometrics?

Ans. If the accused does not comply with a request to furnish access credentials, the Investigating Officer has the option to seek judicial intervention. The officer may approach the court to request necessary directions compelling the accused to provide the required information or to authorize a search of the Smartphone or other electronic devices. Additionally, the Investigating Officer can apply for a search warrant from the court to conduct a lawful search of the electronic equipment in question.

Q3. Can a Court issue a suo moto order directing the accused to provide a password, passcode, or biometrics?

Ans. The Hon'ble High Court highlighted that the process of gathering evidence, including the methods used for investigation, falls within the exclusive domain of the Investigating Officer. Therefore, a court does not have *per se* the authority to independently issue such a directive to the accused. While the court may instruct an accused to cooperate with an investigation, this does not extend to compelling them to disclose access credentials.

Furthermore, the court is not an investigative body and cannot, on its own, mandate the furnishing of a password, passcode, or biometrics. It can only intervene upon receiving a formal application from one of the parties involved in the case.

22 **(Although the Questions raised in this case are maintained herein as they are, however, the observations made by the Hon'ble High Court with regard to those questions are summarized for brevity and easy understanding of readers)**

Q4. What is the consideration for the issuance of a search warrant in order to search a smartphone or computer system or electronic devices?

Ans. In criminal investigations, the search of smartphones or computer systems or electronic devices or records may be necessary under two distinct circumstances:

A. Emergent situations

With regard to emergent situations, the Hon'ble High Court observed that although there is no particular framework provided for search of Electronic Devices but broadly the framework provided under CrPC[23] and to some extent Information Technology Act would be applicable to the searches of electronic devices. The Hon'ble High Court has also observed that in situations when data is going to be immediately destroyed or there is danger of the equipment itself being destroyed or the possibility of equipment not being available, etc the I.O can exercise powers under Section 106 BNSS/ Section 102 CrPC to conduct a warrantless search, however, with certain safeguards mentioned below:

Safeguards for Conducting a Warrantless Search

- There must be **reasonable grounds** to believe that an immediate search is essential to prevent an offense or avoid loss of crucial evidence.

23 **Relevant Provisions of Cr.P.C./B.N.S.S**

- **Section 91(Section 94 B.N.S.S):** Enables a court or police officer to summon a person to produce a document or object relevant to an investigation.
- **Section 92(Section 95 B.N.S.S):** Grants authority to courts (District Magistrate, Chief Judicial Magistrate, Sessions Court, or High Court) to direct postal or telegraph authorities to provide documents or parcels in their custody. Law enforcement officers like the Commissioner of Police or Superintendent of Police can also request such searches.
- **Section 93(Section 96 B.N.S.S):** Allows a court to issue a search warrant under the following conditions:
  - If a person refuses to produce a document or item as required under Section 91.
  - If the document or item is not known to be in anyone's possession.
  - If a general search or inspection is deemed necessary for an inquiry, trial, or other legal proceedings.
- **Section 93(2) (Section 96 B.N.S.S):** Permits the court to restrict a search to a specific location, timeframe, or purpose.
- **Section 94(Section 97 B.N.S.S):** Authorizes certain courts to search places suspected of containing stolen property, forged documents, counterfeit materials, obscene objects, or other prohibited items.
- **Section 100(Section 103 B.N.S.S):** Provides that if a place is locked, the occupant or person in charge must allow entry for a search upon the production of a valid warrant. It also mandates that a search of a woman must be conducted only by another woman.
- **Section 102(Section 106 B.N.S.S):** Grants authority to seize any item found during a search, provided specific conditions are met.
- **Procedure Under Section 165 of Cr.P.C. (Section 185 B.N.S.S)**

- ☐ The Investigating Officer must **record in writing** the reasons for conducting the search without a warrant, providing sufficient detail to justify the urgency.
- ☐ The objective assessment of the emergency must be documented to protect the rights of the individual or organization being searched, particularly considering the **right to privacy**.

B. As part of the regular investigation process.

When a search is required in the normal course of an investigation, as there is usually sufficient time for law enforcement to plan the search methodically. The Investigating Officer may issue a notice under Section 91 of Cr.P.C. (Section 94 B.N.S.S), directing the accused or any other person to produce a specific document or electronic device. If the document or device is not voluntarily provided, the officer may seek a search warrant from the court under Section 93 of Cr.P.C. (Section 96 B.N.S.S).

Once a **search warrant is issued**, the recipient is legally required to:

- ☐ Allow the search to take place.
- ☐ Provide the document or device requested in the warrant.

While highlighting the obligation to allow search subsequent to issue of search warrant, the Hon'ble High Court has also drawn references of Section 100 CrPC (Section 103 BNSS) and observed that applying the principle of S100 CrPC, during search of an electronic equipment the accused person will be required to provide access to password, passcode to unlock the said equipment. Hon'ble High Court has also emphasized upon applicability of Section 69(1)[24] of the IT Act, which grants certain officials the power to issue orders compelling the decryption of data stored, transmitted, or received in a computer resource, including smartphones.

It is important to mention that the Hon'ble High Court has also described the possible contour and scope of search warrant while searching electronic equipments. The relevant paragraph is as follows:

24 **69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.--** (1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

"While issuing a search warrant, ***the concerned Court would have to indicate as to what smart phone, electronic equipment or email account is to be searched.*** *The role of the same in the crime, the nature of search to be done, place where the search has to be done as also specifically interdict the persons carrying out the search from disclosing the material and/or data procured during the course of the said search to a third party. So as to preserve the privacy of the concerned."*

During search and seizure of electronic equipment, the investigating agencies are also required to adhere and observe the well-established and settled procedural safeguard for conducting searches such as presence of lady officer as and when required, disclosing own identification, presence of witnesses and Panchnama, providing copies to the accused and reporting the same to the authorities.

Q 5 . What can be done if the accused or anyone connected to the investigation refuses to provide a password, passcode, or biometrics, even after a search warrant or direction has been issued?

Ans. In such cases, the investigating agency can draw adverse inferences if the accused fails to cooperate, or if they provide incorrect information. The accused should only be given one opportunity to provide the correct password, passcode, or biometrics, as repeated incorrect attempts may result in the device being locked or data being wiped.

If the accused still refuses to cooperate, the investigating agency may engage specialized agencies to crack the password, passcode, or biometrics. The accused cannot contest the methods used to access the device, as they were given a chance to cooperate. The agency may also clone the device or access cloud services linked to it for further investigation and trial purposes.

Furthermore, the investigating agency can block access to the smartphone or email account by changing the password and restricting access to authorized officers. Any data obtained can be preserved and used for the investigation.

To proceed, the prosecution must first seek a search warrant from the court to access the smartphone or email account. If the accused fails to provide the necessary credentials, the agency can serve a notice warning of adverse consequences. If non-cooperation continues, the court may order the service provider or manufacturer to unlock the device. If this fails, the court may allow the agency to hack into the device.

In the event that the data is destroyed during this process, the prosecution may rely on the notice given to the accused about the adverse inference being drawn due to their non-cooperation.

Q 6. **Can the data retrieved from a smartphone or email account alone establish the guilt of an accused person?**

Ans. Hon'ble High Court has observed that, providing password, passcode or biometric access would be akin to operation of Section 161 of Cr.P.C(Section 180 B.N.S.S), Section 160 of CrPC(Section 179 BNSS) and 311-A of Cr.P.C.(Section 349 B.N.S.S). On the point of establishing the guilt of the accessed person on the data so retrieved, Hon'ble High Court has observed that if an accused provides access to a smartphone, email, or other electronic.

Q 7. Does providing a password, passcode, or biometric access to a smartphone or email account constitute self-incrimination or testimonial compulsion?

Ans. It is argued that such actions do not amount to giving testimony, as they simply provide access to data or documents. The **Apex Court's ruling in *Kathi Kalu Oghad's case* (AIR 1961 SC 1808)** clarifies that physical samples (such as fingerprints or thumb impressions) do not amount to testimonial compulsion, and similarly, providing access to electronic devices is not the same as being a witness.

The mere presence of documents or data on a smartphone or email account does not automatically establish guilt or innocence. Both the prosecution and defense must prove the relevance and authenticity of such data with additional evidence.

Accepting the contrary argument would lead to absurd outcomes, such as prohibiting the collection of blood, DNA, or handwriting samples, or even making it impossible to investigate crimes like cybercrime or pornography.

Providing access to a device or account is not the same as answering a question posed by the investigating officer. It is akin to producing a document or a sample, and does not violate **Section 151(2) of Cr.P.C. (Section 170 B.N.S.S)** or involve forced testimony. The prosecution must still prove the relevance of the gathered data using legal procedures and evidence. Thus, such actions do not amount to self-incrimination or testimonial compulsion.

Q 8. Does providing a password, passcode, or biometrics violate a person's right to privacy?

Ans. This question must be evaluated in light of the principles set forth in the ***Justice Puttaswamy case.***[25] The concern arises because smartphones and other electronic devices may contain personal data that is not related to the investigation. Once the investigating agency gains access to such devices, it can view not only the data on the device but also any connected cloud services, which could include sensitive personal, financial, or privileged information.

Unlike physical documents, which can be classified as privileged or confidential, data on a smartphone or electronic device is not compartmentalized. Access to these devices gives

25 (2017) 10 SCC 1

the investigating officer full access to all stored information, including potentially private or incriminating data.

However, using such data during an investigation does not necessarily violate the right to privacy, as long as it falls within the exceptions outlined in the **Puttaswamy case.** Any disclosure or use of such data in court proceedings must be determined by the court through a judicial order. Importantly, the investigating officer is responsible for safeguarding this data and cannot disclose it to any third party without the court's written permission. If this duty is violated, the officer may face disciplinary action.

Q 9. What steps must the investigating officer take to ensure proper handling of smartphones and electronic devices during a search?

Ans. The search must be conducted scientifically and methodically, especially since the data on such devices can be sensitive. There are no specific rules from the police department on how to conduct searches of electronic devices, but it is important that guidelines be developed for this purpose. (**For better understanding readers may refer to page - 56 & 58)**

***Madhukara v. State of Karnataka,* 2018 SCC OnLine Kar 3813 : ILR 2019 Kar 1086 : (2019) 1 KCCR 841 : (2019) 2 Kant LJ 300 at page 1114[India Kanoon - https://indiankanoon.org/doc/36396849/]**

Facts:

On 11th August, 2011, at around 02:00 pm, an elderly woman namely, Basamma (deceased) was found dead in her house situated in Shimogga district of Karnataka. The deceased used to stay with her daughter (Bharti), grand-daughter(Smitha) and son-in-law. It was Smitha who had first seen the deceased after she returned home at around 02:00 pm and accordingly informed all the relatives. Family members of the deceased noticed that some gold ornaments were missing from home and they also noticed blood stains on the bed of deceased. Facts also reveal that deceased had difficulty in walking and at the time of alleged incident she was alone at her home. The Police of Vinob Nagar Police Station, Shimogga registered a case as per the allegations made by complainant granddaughter (Smitha) in Crime No. 127/2011 for the offence punishable under Section 302 and 397 of IPC and took up the investigation, against Madhukara(A1) and Malyappa(A2).

During investigation case was found true against two individual Madhukara (A1) and Malyappa (A2); and they were prosecuted for charges under Sections 302 (murder) and 397 (robbery with murder) of the Indian Penal Code (IPC). Madhukara (A1) stood convicted under Section 302 and 397 IPC whereas Malyappa(A2) was acquitted.

In appeal before the Karnataka High Court, although both the accused stood acquitted, the Hon'ble High Court made and observation/ guidelines regarding collection and presentation of electronic evidences. The Hon'ble Court made the observation in context of the fact that *one of the material exhibits presented by prosecution was a compact disc(CD) containing video footage of place near the area of the house of the deceased, but during appeal the said CD(file) could be played only twice and on a subsequent occasion the file did not open, apparently because the said CD was stitched by the office of the Trial Court.* While observing this fact, the Hon'ble High Court made some observation, guidelines with regard to collection and presentation of electronic evidence which are summarized below:

A. **Direction to Trial Courts**

(i) After admitting the electronic evidence, trial courts must take utmost care to preserve the electronic evidence intact, till the case is logically concluded;

(ii) **Preserving the electronic medium/ evidence at the Ministerial Office of the Court:** The electronic media should be kept in safe deposit with the Ministerial Office of the Court with a direction to preserve it in proper manner till the case is logically concluded.

(iii) **Maintaining Simultaneous copy** at the Server/Personal Computer of the Police Station or Investigating Officer as well as the Computer of the Court concerned.

B. **Direction to Investigating Officers**

(i) **To preserve electronic evidence from moisture and humidity:** Investigating Officers have to preserve electronic evidence in proper manner and keep them in custody in an anti-static envelope, away from humidity, heat etc;

(ii) **Seizure & transmission of electronic evidences:** To take proper precautions for search, seizure, packing, labeling, sending the digital evidence to expert, submitting to the Trial Court with proper custody in sealed and secured manner.

(iii) **Removable/Disable security settings:** Investigating Officer has to make efforts to disable security settings like PIN, Password, Pattern Lock, Finger Print etc., before seizure procedure so that it should not create further obstruction/hurdle at any stage for the purpose of perusal, analysis of electronic gadgets.

(iv) **Retention of a copy:** Investigating Officers should also retain a copy of the said evidence so that in the circumstances of the destruction or corruption of original one, the copy so made can be put up as secondary evidence.

(v) **Safety from damage due to packing: I**t has to be ensured that such media do not get damaged due to the packing, sustain scratches (if optical) in any way while handling the file.

(vi) **Use of anti-static envelope:** The media viz., CD/DVD/Pendrive/Hard Disk/ Magnetic device etc., should be preserved in antistatic envelope, away from humidity and heat in a proper manner even before the same is produced before the Court.

(vii) While searching personal computers or laptops, a qualified forensic examiner should accompany the search team. Investigating officers should not operate the computers or search the data themselves.[26]

(viii) If the device is powered on, the officer must avoid turning it off and instead secure the services of a forensic expert to capture volatile memory data. If the device is powered off, it should remain off, and a photograph of its connections should be taken.

(ix) If the device is part of a network, the officer should ensure the seizure of any connected remote storage devices, routers, modems, and any wireless access points that might have been used.

(x) In the case of mobile devices, further precautions include preventing the device from communicating with networks by placing it in a faraday bag, keeping it charged, and removing the SIM card.

(xi) The officer should also document the entire process, from the entry into the premises to the exit, ensuring all steps are recorded for legal integrity. These measures ensure that the evidence remains secure and the investigation proceeds in a legally compliant manner.

C. **Direction to Government Authorities, FSL, etc.**

(i) Direction to Government Authorities: Proper training to the investigating officers and also the concerned staff, Judicial officers and staff of the Court with reference to packing and preserving the media for future use and retrieval of the contents of the said electronic media, as and when required, so that it would safely exist till the case is logically concluded.

26 Point number **vii to xi** are from ***Virendra Khanna v. State of Karnataka*, 2021 SCC OnLine Kar 5032,(**some additional guidelines have been noted by the Hon'ble High Court)

(ii) **Retaining a copy by the FSL:** Experts at FSL also if possible have to retain a copy of mirror image, extracted data with evidentiary value with proper labeling, which may be used as a secondary evidence at any point of time.

Chapter 3. Technical Know How of Cyber Technology: Hash Value and Cloud Computing

3.1 HASH VALUES

Hash values serve as unique electronic fingerprints in digital forensics, playing a crucial role in maintaining evidence integrity during legal investigations. When digital forensics professionals generate these cryptographic representations of files, they establish an unalterable reference point that serves multiple legal purposes.

The primary legal significance of hash values lies in their ability to verify evidence integrity. During investigations, numerous tools and analytical techniques are applied to digital evidence, and hash values provide a reliable method to demonstrate that the original data remains unaltered. This is particularly important for meeting legal standards of evidence admissibility and chain of custody requirements.

In the context of legal proceedings, hash values facilitate secure information sharing among various parties. When electronic documents are distributed to attorneys, experts, or other stakeholders, hash values serve as mathematical proof that all parties are working with identical copies of the evidence. This helps prevent disputes about document authenticity and ensures consistency throughout legal proceedings.

Hash values also play a vital role in managing electronically stored information (ESI) during legal discovery. They enable efficient identification and filtering of duplicate files, including emails, attachments, and other electronic documents. Additionally, hash values verify the accuracy of forensic images or clones, ensuring that exact copies of digital evidence are preserved for legal examination.

Hashing as per Jharkhand Police – Cyber Crime Investigation Manual[27]

- A reliable Hash proves that media contents have not been altered
- Hashing program produces a fixed length large integer value (ranging from 80-240 bits) representing the digital data on the seized media.

27 Jharkhand Police: Cyber Crime Investigation Manual, https://jhpolice.gov.in/downloads/cyber-crime-investigation-manual-dsci-file-size-135-mb-32514-1512041410, Last accessed on 15.02.2025

- In case if there is an alteration to the original evidence, there will be a consequent change to its hash value.
- The process of Hashing is applying a mathematical algorithm to a file/disk/storage media to produce an unique value which is akin to a fingerprint, thus, any changes in data results in change of the Hash value.
- It is one of the most widely accepted methods of authenticating any given data in the courts of law.
- Hash value is usually a combination of alphabets and numbers.
- There are different types of Hash algorithm; MD5 (Message Digest 5), SHA256 (Secure Hash Algorithm).

Relevant Guidelines Related to Hash Value

Relevant Provision of IT Act: Section 3 of the IT Act - Authentication of Electronic records mention that:.

(1) X X X

(2) The authentication of the electronic record shall be effected by the use of an asymmetric cryptosystem and hash function which envelopes and transforms the initial electronic record into another electronic record.

Explanation.- For this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

The hashing algorithm has some unique characteristics, which are as follows:

1. Message digest always of a fixed length: The digital evidence may be of any size, but on application of the hash algorithm the resultant message digest would always be of a fixed length.
2. Message digest is a uniquely generated number: The message digest is a unique number generated by a hash function from a set of data. If the contents of the digital evidence

remain the same, the hash function would generate the same message digest every time it is applied to the digital evidence. This property is useful in authenticating seized digital evidence before a court of law. If application of the hash function on digital evidence in a court of law results in the same message digest as was obtained during the time of seizure, it indicates that the presented evidence is the same as what was seized.

3. One-way hash function: It is computationally not feasible to determine the contents of the digital evidence if somebody knows the message digest. Hash algorithm is a one-way function. This property is of great importance from the legal point of view, since it prevents manipulation of digital evidence as no one can predict the message digest that would be generated if the evidence is manipulated.

The Bharatiya Sakshya Adhiniyam, 2023 (BSA) replaces the Indian Evidence Act, 1872, introducing significant changes in the admissibility of electronic evidence to align with technological advancements. It replaces the procedure under Section 65B of the old Evidence Act with a new system under Section 63 of the BSA.

Under the BSA (formerly Indian Evidence Act), Section 63 now governs electronic evidence admissibility, modifying the certification process. The certificate is divided into two parts: Part A, to be filled by the party submitting the evidence, and Part B, which must be completed by an 'expert' as defined under Section 63(4)(c) as *"an expert shall be evidence of any matter stated in the certificate."*

This 'expert' means any other person with necessary expertise who has to fill in the details of the electronic record. The new procedure under this form is filling in of *hash function* of the electronic evidence being submitted (as shown below).

PART B

(To be filled by the Expert)

I, _____ (Name), Son/daughter/spouse of _____ residing/employed at _____ do hereby solemnly affirm and sincerely state and submit as follows:—

The produced electronic record/output of the digital record are obtained from the following device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: _____

Make & Model: _____ Color: _____
Serial Number: _____
IMEI/UIN/UID/MAC/Cloud ID _____ (as applicable)
and any other relevant information, if any, about the device/digital record _____ (specify).

I state that the HASH value/s of the electronic/digital record/s is _____, obtained through the following algorithm:—

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other _____ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

(Name, designation and signature)

Date (DD/MM/YYYY): _____

Time (IST): _____ hours (In 24 hours format)

Place: _____

The hash function value mentioned in Part B of the certificate under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, is a cryptographic identifier attached to electronic documents and websites. It ensures data integrity and verifies that electronic records remain unaltered. This addition aims to enhance the reliability, accountability, and efficiency of electronic evidence in the justice system.

The extraction of the hash function is a newly introduced technical requirement under the BSA. The process involves specific steps to generate and verify the hash value of an electronic record, ensuring compliance with the new evidentiary standards.

Step by Step Guide to Extract Hash Function Value from Electronic Evidence[28]

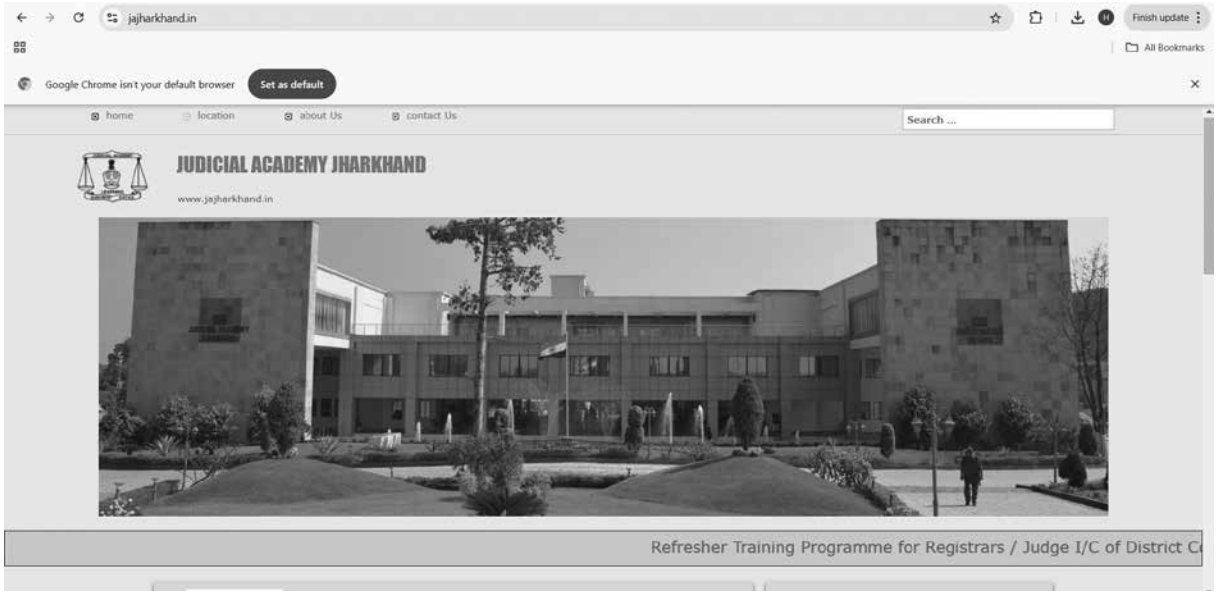
Extraction of Hash Function Value

The Digital Evidence Investigation Manual Central Board of Direct Taxes, Department of Revenue, Ministry of Finance, Government of India may be reffered regarding extraction of hash values. The said rules are available at:

https://nadt.gov.in/writereaddata/MenuContentImages/digital-evidence-investigation-manual-201463853204547545422O.pdf

1) *From a website (SHA format as required in Part B of the Schedule of BSA): For convenience of readers an example of the website of the judicial academy has been taken.*

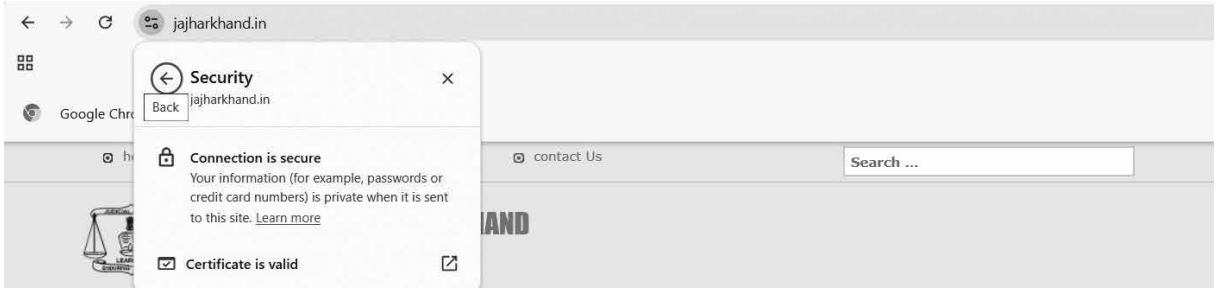
   a) *Open the website from where the hash function value needs to be extracted*



28 https://www.barandbench.com/law-firms/view-point/tech-savvy-evidence-system-step-by-step-guide-hash-function-value-electronic-evidence

b) Click on the lock button and open the connection details appearing on left side of the search bar (the lock is depicted in the below-mentioned picture)

c) Open the digital certificate of the website after clicking at connection is secure, click the certificate is valid (as depicted in below-mentioned photograph)

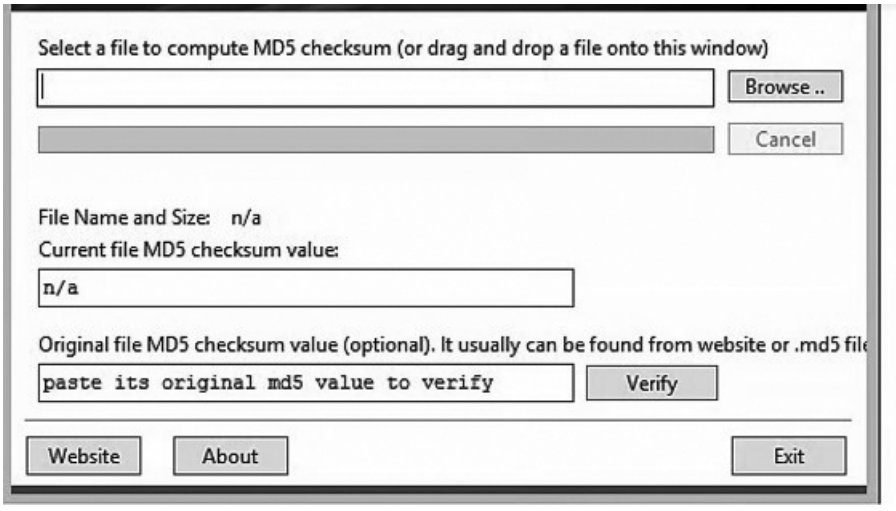


d) The hash value of the website will appear in the certificate in SHA format which can be copied directly (SHA certificate is in the yellow colour box depicted below)

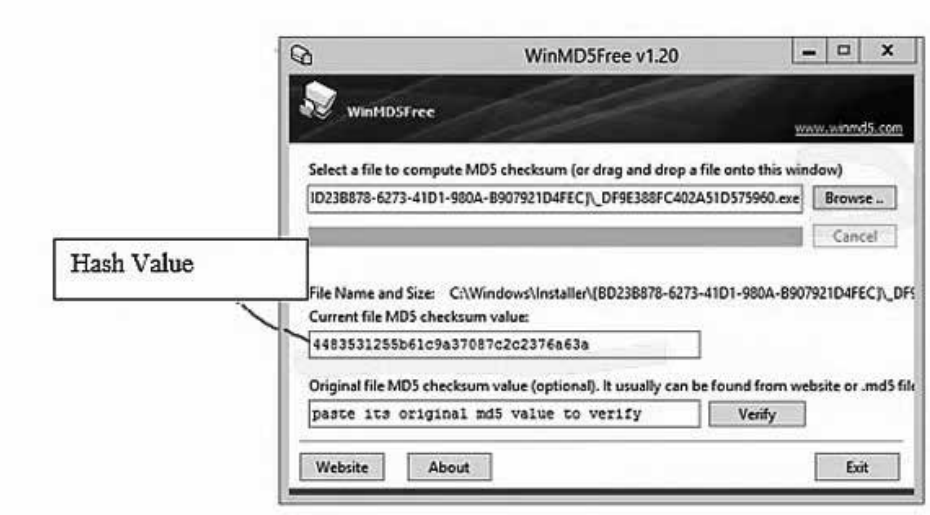
2) From any offline file (MD5 Format)

a) Download an application under the name of WINmd5 from google chrome.

b) Open the downloaded file and run the application.



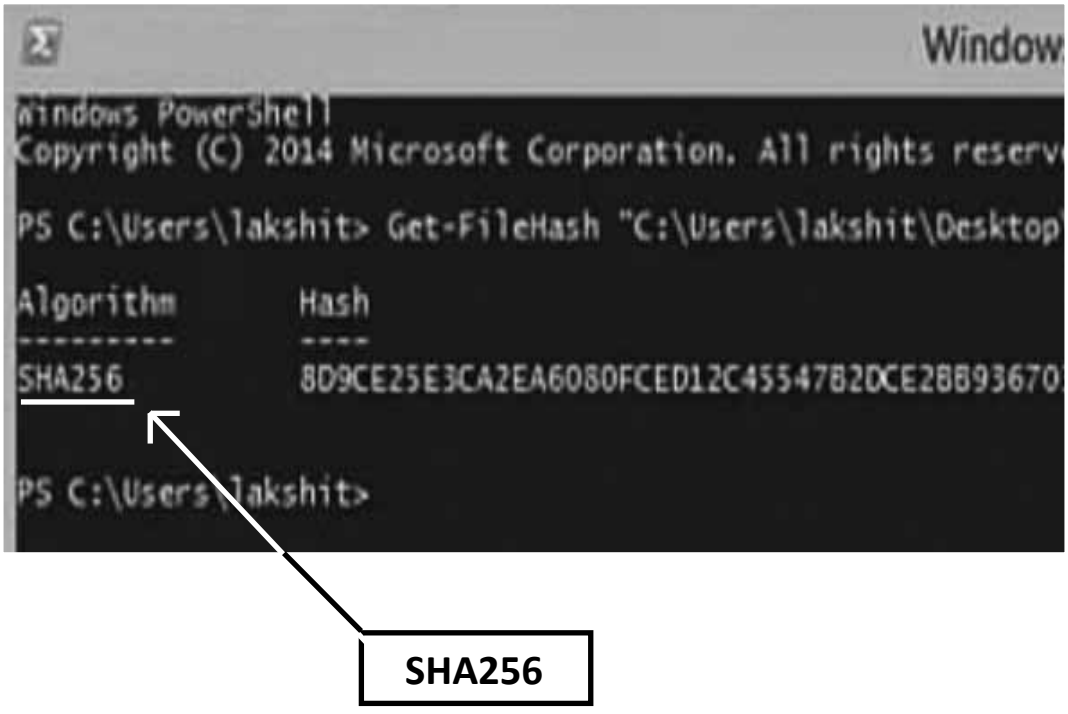
c) Drag and drop file the file whose hash value has to be extracted or select the file from the browse menu from file explorer and the MD5 hash value will appear.



Alternatively- (SHA 256 format)

1) To extract hash value in SH256 format of an offline file -open Windows Power Shell from start menu of Windows Computer:

2) Enter command "Get – FileHash" followed by a space. Drag the downloaded file or installer onto the Windows PowerShell window after the Get – FileHash command and the space. Alternatively, enter the full path to the file or installer in double quotes after the space and press Enter key



Challenges in Ascertaining Hash Values Under the BSA

The inclusion of hash functions in electronic evidence aims to enhance reliability, but several challenges persist:

1. **Multiplicity of Documents** – In cases like trademark infringement, hundreds of electronic documents may be presented, each requiring unique hash values. Extracting and verifying all of them is a complex process.

2. **Deletion of Evidence** – Another challenge occurs when evidence is collected without extracting the hash value, and a notice is sent to the accused party before filing the suit. If the evidence is deleted before the suit is led, the hash value cannot be extracted from the original source.

3. **Verification of Old Evidence** – Many old electronic records lack original sources, making hash extraction unfeasible, particularly in cases requiring proof of prior use.

4. **Awareness and Infrastructure Gaps** – Technical knowledge about hash extraction is limited, especially outside metropolitan areas, affecting effective implementation.

5. **Authorization of Experts** – The Act lacks clarity on who qualifies as an "Expert" to certify hash values, leading to uncertainties in the certification process.

Way Forward

To address these challenges, the following steps should be considered:

- **Establish Clear Guidelines** – Regulatory bodies should collaborate with industry experts to standardize hash functions and create clear compliance frameworks.

- **Standardized Hash Functions & Updates** – Define and periodically update a list of approved hash functions to maintain security and adaptability.

- **Training & Awareness** – Conduct legal and technical training programs for stakeholders, including legal professionals, to ensure smooth implementation.

- **Guidance Documentation** – Publish resources outlining best practices and common pitfalls in hash value certification under Section 63(4).

- **Technological Solutions** – Develop automated tools for hash value extraction and verification to streamline compliance efforts.

3.2: CLOUD COMPUTING

What is Cloud Computing-

Cloud computing is a model of convenient and on-demand access and availability to computer resources especially data storage and computing power which is supplied with minimal direct and active management by the user and nominal amount of effort from the service provider.[29]

The United States National Institute of Standards and Technology (NIST) had released the first and widely acceptable definition of cloud computing by identifying its main characteristics which had been submitted as the U.S. Contribution to international standardization and according to this definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Core Issues with Cloud Computing [30]

(i) Privacy Concerns – It represents one of the foremost challenges in cloud computing, encompassing both data security and jurisdictional complexities. The legal framework governing cloud service providers requires adherence to both international standards and local laws where servers are located. While basic security standards are mandatory, they don't guarantee complete protection. Data storage options include both encrypted and unencrypted forms, each carrying distinct legal implications. In India, government access to cloud data is facilitated through several legislative provisions. The Information Technology Act, 2000, particularly Sections 69 and 69-B, empowers authorized agencies to access, intercept, and decrypt data. Additionally, Section 91 of the Criminal Procedure Code (**Section 94 BNS)** enables government authorities to access sensitive cloud-stored data. While these interferences are done through lawful procedures, they can be easily misused by authorities and data can be accessible for purposes that do not strictly pertain to law-and-order concerns.

(ii) Cyber Crimes and Cloud Security - The evolution of cybercrime in cloud computing has introduced increasingly sophisticated attack methods. Crypto – Jacking is one such methods.

29 Paul M Schwart, 'Information Privacy in the Cloud' (2013) 161 (6) University of Pennsylvania Law Review

30 Cloud Computing and Challenges Faced in Existing Legal Structure by Divyaraj Ray, 2.1 JCLJ (2021) 483

(iii) Loss of Data - Data loss liability in cloud computing operates under a shared responsibility model, creating complex liability situations. Service providers bear responsibility for cloud infrastructure security, while end-users remain liable for the content of stored data. Notably, providers typically offer no automatic compensation for data loss.

(iv) Jurisdictional Issue - The multi-jurisdictional nature of cloud services creates significant legal complexities. These services typically operate across multiple jurisdictions with varying international standards, creating substantial enforcement difficulties across borders. Subcontracting arrangements further complicate these jurisdictional issues. Different regions have adopted varying approaches to address these challenges. This jurisdictional complexity remains one of the most significant challenges in cloud computing law, requiring careful consideration in both contract formation and dispute resolution.

Legal Framework Regulating Cloud Computing in India

India's approach to cloud computing regulation is characterized by a composite framework of general cyberlaws and sector-specific regulations, rather than dedicated cloud-specific legislation like the EU's Cloud Act. The primary legislative foundation rests on the Information Technology Act, 2000, supplemented by various rules and regulations that collectively govern the cloud computing space.

Primary Legislative Framework

The Information Technology Act, 2000 serves as the cornerstone legislation, providing indirect regulation of cloud services through its broader governance of cyberspace. This is complemented by two crucial implementing rules:

1. Information Technology (Reasonable security practices and procedure and sensitive personal data or information) Rules, 2011

2. Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013

Key Provision of IT Act:

Section 43-A[31] of the Information Technology Act, 2000 provides the most direct regulation of cloud computing services. This section specifically addresses corporate entities and e-businesses

31 [43A. Compensation for failure to protect data.–Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected

that utilize cloud services and make them available to end-users, particularly those handling sensitive information. The provision establishes a compensation mechanism whereby corporate bodies can be held liable for negligent security practices that result in wrongful loss or gain to any person.

Chapter 4. Electronic or Digital Evidence

4.1 INTRODUCTION

The term "electronic or digital evidence" is not explicitly defined in either the Indian Evidence Act, 1872, or the Information Technology Act, 2000, however, the Explanation attached to **Section 79A of IT Act** defines "electronic form evidence" as: *"any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones and digital fax machines."*.

Further, it is important to mention that in the Bharatiya Sakshya Adhiniyam there are explicit references/ use of the term "electronic or digital records"; "statements given electronically" etc. In the definition clause of BSA the term "Document" (Section 2(d), BSA)[32] and "Evidence" (Section 2(e), BSA)[33] are expanded to include "electronic or digital record" as well. Additionally, oral evidence under Section 2(e), BSA also expands its definition to include statements given electronically.[34] Prior to enactment of BSA, 2023, Section 3 of IEA, did not include statements given electronically. Hence, it is evident that even the BSA does not explicitly defines "electronic or digital evidence".

The **Information Technology Act, 2000**, provides definition of electronic record. **Section 2(t)** defines "electronic record" as *"data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche."*[35]

32 *Section 2(d), BSA: ""document" means any matter expressed or described or otherwise recorded upon any substance by means of letters, figures or marks or any other means or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter and includes electronic and digital records."*

33 *Section 2(e), BSA: "(ii) all documents including electronic or digital records produced for the inspection of the Court and such documents are called documentary evidence"*

34 Section 2(e), BSA: "(i) all statements including statements given electronically which the Court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry and such statements are called oral evidence"

35 Section 2(o), IT Act further defines "data" as: "a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer."

4.2 ADMISSIBILITY, PROVING AND APPRECIATION OF ELECTRONIC OR DIGITAL EVIDENCE

Earlier the Indian Evidence Act, 1872 did not contain any provision dealing with electronic record or digital evidence and its admissibility or proving. However, with the advancement of science and technology the need for such provision had led to the insertion of **Section 65A and Section 65B** in the IEA under the Chapter "***Of Documentary Evidence***", introduced through Information Technology Act, 2000, to address the admissibility of electronic record. The above provisions of IEA also find its place in the newly enacted Bharatiya Sakshya Adhiniyam, 2023 with an addition that the provisions dealing with admissibility of "electronic record" is also expanded to include digital record which is evident from wordings of Section 61 of BSA. The BSA introduces **Section 61**, which ensures that the admissibility of "*electronic or digital records*" as evidence cannot be denied solely on the grounds of their digital nature and subject to operation Section 63, such records are granted the same legal effect, validity, and enforceability as other documents.[36]

A reading of Section 63 of BSA (Section 65B, IEA) provides that an output of electronic record saved or stored in electronic form but subsequently printed on a paper or produced by computer would fall under the category of "document". Further, in order to make it admissible Section 63, BSA (Section 65B IEA) itself outlines the principle conditions including mandatory certification of such "document" while doing away with requirement of further proof or production of the original. Statutorily, when electronic records are submitted as evidence in the court, they are deemed as "documents" under the BSA.

Where a statement in evidence is sought to be given by virtue of Section 65B, Section 65B(4) states that a certificate needs to be presented that recognizes the electronic record having the statement and explains the way in which it is to be presented, and gives particulars of the device involved in the production of the electronic record to show that the electronic record was produced by a computer, either by a person occupying a responsible official position in relation to the operation of the relevant device, or the management of the relevant activities, whichever is appropriate.

36 Section 61, BSA: "*Electronic or digital record.— Nothing in this Adhiniyam shall apply to deny the admissibility of an electronic or digital record in the evidence on the ground that it is an electronic or digital record and such record shall, subject to section 63, have the same legal effect, validity and enforceability as other document.*"

4.3 TRAJECTORY OF SECTION 63 BSA [65-B IEA]: *STATE OF NCT DELHI V. NAVJOT SANDHU* TO *ARJUN PANDITRAO KHOTKAR V. KAILASH KUSHANRAO GORANTYAL*

Sections 65A and 65B also serve as an exception to the general rule of evidence where a litigating party is expected to bring original document. Section 65A and Section 65B may fall in the category of exception because Section 65B recognises electronic evidence as "deemed document" and at the same time with a shield and protection of Section 65B(4) saves the litigant/ the party submitting electronic record, from the rigour of proving it to be original document. However, Section 65B (4) does not explicitly state the stage at which it should be presented.

Through various judgments, the Supreme Court has endeavoured to clarify the legislative intent behind these provisions. There have been multiple litigations over the scope and ambit of Section 65B, with divergent views taken by the Supreme Court. Confusion arose over the scope and ambit of Section 65B as inconsistent views had been taken in four earlier decisions of the Supreme Court – in ***State (NCT of Delhi) v. Navjot Sandhu***, [(2005) 11 SCC 600], ***Anvar P.V. v. P.K. Basheer***, [(2014) 10 SCC 473], ***Tomaso Bruno v. State of Uttar Pradesh***, [(2015) 7 SCC 178], and ***Shafhi Mohammad v. State of Himachal Pradesh***, [(2018) 2 SCC 801]. In a decision delivered on July 14, 2020, a three-judge bench of the Supreme Court, in ***Arjun Panditrao Khotkar v. Kailash Kishanrao Goratyal***, [(2020) 7 SCC 1] has now finally clarified the interpretation of Section 65B.

***State (NCT of Delhi) v. Navjot Sandhu*, [(2005) 11 SCC 600]**

The two judge bench held that irrespective of the compliance of Section 65B, electronic record could be admitted as secondary evidence under Sections 63 and 65.

***Anvar P.V. v. P.K. Basheer,* [(2014) 10 SCC 473]**

The three judge bench overruled the Supreme Court's view regarding electronic record in the ***Navjot Sandhu case*** and held that Section 65B is a special provision to admit electronic record as secondary evidence. However, electronic record can be admitted as a primary evidence under Section 62.

***Tomaso Bruno v. State of Uttar Pradesh*, [(2015) 7 SCC 178]**

The three judge bench cited ***Navjot Sandhu case*** to discuss the relevance of electronic evidence, despite it being overruled.

***Shafhi Mohammad v. State of Himachal Pradesh,* [(2018) 2 SCC 801]**

The two judge bench differed from the judgement of ***Anvar P.V case*** and held that Sections 65A and 65B cannot be held to be a complete code for admissibility of electronic records. And in cases where the party submitting the electronic evidence is not in possession of the device, the requirement of certificate under Section 65B can be relaxed.

***Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal*, [(2020) 7 SCC 1]**

The three judge bench upheld the judgement of ***Anvar P.V case***, in addition to that overruled the clarification regarding Section 65B given in ***Shafhi Mohammed case*** and overruled the judgement in ***Tomaso Bruno*** case as per incuriam. The court held that the certificate under Section 65B is mandatory and condition precedent for admissibility of electronic evidence.

1. *State (NCT of Delhi) v. Navjot Sandhu*, [(2005) 11 SCC 600] [Famously known as the *Parliament Attack Case*]

This is amongst the few landmark cases wherein the issue related to interpretation and necessity of certificate under Section 65B, IEA was deliberated upon. One of the major issues raised for consideration by the accused in the appeal was regarding admissibility of the electronic records which were mobile phone call records produced by the prosecution.

The counsel, on behalf of the accused, challenged the credibility and reliability of the call records produced by the prosecution. The counsel argued that the prosecution had failed to produce a certificate mandated under Section 65B (4) of the Indian Evidence Act, which is essential for admitting electronic records as evidence. They further argued that in the absence of the certificate mandated under sub-Section (4) of Section 65B of the Indian Evidence Act, the information provided by the electronic record cannot be adduced in evidence. In absence of a "competent" witness accustomed with the functioning of the computers during the time printouts were taken the secondary evidence under Section 63 is also inadmissible.

The Supreme Court, however, concluded that the cross-examination of competent witness who was familiar with the functioning of the computer during the relevant time and the manner in which the printouts of the call records were taken was sufficient to prove the call records. While considering the printouts of the computerized records of the calls pertaining to the cell phones, it was held at Paragraph-150 as follows:

"150. According to Section 63, secondary evidence means and includes, among other things, "copies made from the original by mechanical processes which in themselves insure the accuracy of the copy, and copies compared with such copies". Section 65 enables secondary evidence of the contents of a document to be adduced if the original is of such a nature as not to be easily movable. It is not in dispute that the information contained in the call records is stored in huge servers which cannot be easily moved and produced in the court. That is what the High Court has also observed at para 276. Hence, printouts taken from the computers/servers by mechanical process and certified by a responsible official of the service-providing company can be led in evidence through a witness who can identify the signatures of the certifying officer or otherwise speak of the facts based on his personal knowledge. Irrespective of the compliance with the requirements of Section 65-B, which is a provision dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely, Sections 63 and 65. It may be that the certificate containing the details in sub-section (4) of Section 65-B is not filed in the instant case, but that does not mean that secondary evidence cannot be given even if the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely, Sections 63 and 65."

The Supreme Court thus held that electronic evidence (in this case computer printouts of call records) would fall under the category of secondary evidence under Sections 63 and being secondary evidence the manner of proving the secondary evidence as mandated under Section 65 of the Evidence Act would apply. Thus, Supreme Court essentially done away with requirement of Certificate under Section 65B, IEA in case of electronic evidence.

This ruling regarding applicability of Sections 63 and 65 of IEA with regard to electronic record was overruled by the Supreme Court in the case of ***Anvar P.V v P.K Basheer***, 2014.

2. *Anvar P.V. v. P.K. Basheer*, [(2014) 10 SCC 473]

After the decision of the Supreme Court in ***State (NCT of Delhi) v. Navjot Sandhu,*** 2005, the above judgement by Hon'ble Supreme Court is another important ruling wherein the necessity of certificate under Section 65B of IEA was discussed and decided by the Hon'ble Supreme Court. In this case the earlier view of the Supreme Court that electronic record would fall under the category of Secondary evidence and thus be guided by Section 63 and 65 of IEA, was overruled. ***Anvar P.V v P.K Basheer***, 2014 laid down a uniform practice with regard to admissibility of electronic evidences and mandated one particular method of practice.

In this case, question was raised on the validity of the general election. The appellant contended that during election propaganda the agent of the respondent with the consent and knowledge of the respondent printed allegations of the appellant in a leaflet of at least twenty five thousand copies and also during election propaganda the respondent made objectionable songs and announcements which amounts to commission of corrupt practice under the Section 100(1)(b) of The Representation of the People Act 1951. In the list of evidences, the electronic evidences in the form of CD which were speeches, songs and announcements recorded using other instruments by feeding them into a computer were submitted as an evidence.

The respondent contended that there was no proper fulfilment of requirements under Section 65A and 65B of the Indian Evidence Act, 1872 with regard to evidences adduced by the appellant. Thus, the election is not void under Section 100(1)(b) of the Representation of People Act.

The Supreme Court while dealing with the electronic records, which the court believed to be the major thrust in the arguments, held that any documentary evidence by way of an electronic record under the Evidence Act, in view of Sections 59 and 65A, can be proved only in accordance with the procedure prescribed under Section 65B, IEA.

While overruling the law declared in ***Navjot Sandhu case***, the Apex Court held that Section 65B is a special provision, specifically dealing with electronic evidence. The language of the Section starts with a non-obstante clause thereby overruling the application of any other provision for

determining the admissibility and validity of electronic evidence. The Court applied the maxim of "*Generalia specialibus non derogant*", meaning such special law will always prevail over the general law. Thus, if any electronic record is not made admissible under Section 65B, it cannot be presented under Sections 63 and 65 for they have no application in the case of secondary evidence by way of electronic records.

The three judge bench observed in Para 22 that:

"22….. It appears, the court omitted to take note of Sections 59 and 65A dealing with the admissibility of electronic record. Sections 63 and 65 have no application in the case of secondary evidence by way of electronic record; the same is wholly governed by Sections 65A and 65B. To that extent, the statement of law on admissibility of secondary evidence pertaining to electronic record, as stated by this Court in Navjot Sandhu case (supra), does not lay down the correct legal position. It requires to be overruled and we do so. An electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements Under Section 65B are satisfied. Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible."

The Hon'ble Apex Court also made an important observation with regard to situation if an electronic record is used as primary evidence under Section 62 of IEA. While highlighting and clarifying this the Apex Court held that in situations when an electronic record is used as a primary evidence under Section 62 of IEA, the same would be admissible in evidence without compliance with the conditions stipulated under Section 65B of IEA.

3. *Tomaso Bruno v. State of Uttar Pradesh*, [(2015) 7 SCC 178]

The case concerned an appeal by two Italian nationals who were convicted for the murder of another Italian national during their trip to Varanasi. The Trial Court had convicted the accused on the basis of oral testimony while recognizing the fact that CCTV footages were not brought in evidence by the prosecution. Even the Hon'ble High Court accepted the line of reasoning of trial court and conviction was upheld.

In the appeal before the Supreme Court the contention by defence was that the prosecution has failed to bring in CCTV footages and conviction solely on the oral testimonies, in the factual matrix of this case is legally not tenable and liable to be set aside.

The Hon'ble Apex Court treated the failure to produce the CCTV footage as a material suppression of evidence. While invoking Section 114(g) of the Indian Evidence Act the Apex Court drew an adverse inference against the prosecution due to its failure to produce CCTV footage. Upon

consideration of the facts and circumstances of the case, the Hon'ble Apex Court held that the circumstances and the evidence adduced by the prosecution do not form a complete chain pointing to the guilt of the accused and the benefit of doubt was given to the accused and the conviction of the Appellants was set aside.

The Court, unfortunately, cited ***State (NCT of Delhi) v. Navjot Sandhu*** as precedent, despite this case being expressly overruled by the Supreme Court in ***Anvar P.V. v. P.K. Basheer & Ors.*** The reference of the ***Navjot Sandhu case*** is particularly misplaced, as it pertains to the admissibility of electronic and scientific evidence under Section 65B of the Indian Evidence Act. This oversight undermines the Court's reasoning, given that the ***Anvar*** judgment clarified and reinforced the evidentiary requirements for electronic records, which would have been critical in this case.

4. *Shafhi Mohammad v. State of Himachal Pradesh*, [(2018) 2 SCC 801]

An appeal was filed wherein the key issues involved the necessity of videography of crime scene in every such case of recovery when possession itself is an offence. The submissions emphasized the practical challenges of securing certificates for electronic evidence, particularly when the party seeking to present such evidence does not control the original device. The Court referred to prior judicial pronouncements addressing the procedural requirements for the admissibility of electronic evidence in **Tomaso Bruno v. State of Uttar Pradesh and Anvar P.V. v. P.K. Basheer**, to examine the applicability and scope of Section 65B in such circumstances.

However, the two judge bench deferred from the judgement of **Anvar P.V. v. P.K. Basheer,** and held that Section 65A and 65B are clarificatory and procedural in nature and cannot be held to be a complete code on the subject. The Court further held that irrespective of the compliance with the requirements of Section 65-B, which is a provision dealing with admissibility of electronic records, it does not preclude the introduction of secondary evidence under other provisions of the Indian Evidence Act, such as Sections 63 and 65.

The Court noted that if a certificate under sub-section (4) of Section 65-B is not filed, that would not mean that secondary evidence will be precluded even if the law permits admission of such evidence under Sections 63 and 65 of IEA. The Court emphasized that excluding authentic evidence solely due to the inability to procure a certificate under Section 65B(4) of the Evidence Act, particularly when the party producing the evidence cannot reasonably obtain such a certificate, would amount to a denial of justice. Consequently, the Court unequivocally held that even if the requirements under Section 65B (4) were not satisfied, evidence could be produced under Sections 63 and 65 of the Indian Evidence Act, 1872.

The Supreme Court stated:

"*14. The applicability of procedural requirement Under Section 65B(4) of the Evidence Act of furnishing certificate is to be applied only when such electronic evidence is produced by a person who is in a position to produce such certificate being in control of the said device and not of the opposite party. In a case where electronic evidence is produced by a party who is not in possession of a device, applicability of Sections 63 and 65 of the Evidence Act cannot be held to be excluded. In such case, procedure under the said Sections can certainly be invoked. If this is not so permitted, it will be denial of justice to the person who is in possession of authentic evidence/witness but on account of manner of proving, such document is kept out of consideration by the court in absence of certificate under Section 65B(4) of the Evidence Act, which party producing cannot possibly secure. Thus, requirement of certificate under Section 65B(h) is not always mandatory.*

15. Accordingly, we clarify the legal position on the subject on the admissibility of the electronic evidence, especially by a party who is not in possession of device from which the document is produced. Such party cannot be required to produce certificate under Section 65B(4) of the Evidence Act. The applicability of requirement of certificate being procedural can be relaxed by Court wherever interest of justice so justifies."

The effect of the above two paragraphs apparently indicate that, rigour of submitting certificate under Section 65B is relaxed in such circumstances of admissibility of electronic evidence when a party who is submitting the electronic evidence is not in possession of the device from which the document is produced.

5. *Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal*, [(2020) 7 SCC 1]

Two election petitions were filed by the present Respondents under Sections 80 and 81 of the Representation of the People Act, 1951, challenging the election of the Appellant. The Respondents argued that the returned candidate had filed their nomination forms after the stipulated deadline, thereby rendering the nomination invalid as it was not filed in accordance with the law and should have been rejected. Respondents relied on video-camera arrangements made both inside and outside the office of the RO.

The High Court ordered the Election Commission and the concerned officers to produce the entire record of the election of the Constituency, including the original video recordings. A specific order was made that this electronic record needs to be produced along with the 'necessary certificates'.

The High Court held that the CDs produced by the Election Commission could not be treated as the original record hence, there will be requirement of certificate under Section 65B (4), IEA. After this while perusing the certificate so submitted the Hon'ble High Court referred to the judgment of ***Anvar P.V. v. P.K. Basheer***, and observed that no written certificate, as is

required under Section 65B(4) of the Indian Evidence Act, 1872, had been furnished by the election officials, more particularly the RO. However, the Hon'ble High Court also observed that the certificate so submitted was substantial compliance of Section 65B of IEA. Instead, they would have to be proved through secondary evidence in accordance with the provisions of the Evidence Act.

The Supreme Court upheld the impugned judgment as Bombay High Court relied upon other evidence as well, apart from the evidence in the form of electronic record, to arrive at the conclusion.

The Supreme Court while interpreting Section 65B, upheld the judgment in ***Anvar P.V.*** and overruled the 'clarification' in ***Shafhi Mohammed***. The Supreme Court also overruled the judgment in ***Tomasa Bruno*** which was per incuriam and held that the requirement of certificate under Section 65B is not always mandatory, but a condition precedent to the admissibility of evidence by way of electronic record. The Supreme Court made the following observations:

- The Court reaffirmed that the principles laid down in ***Anvar P.V.*** do not require reconsideration. However, the Court suggested that the last sentence in paragraph 24 of the said judgment which reads as "*if an electronic record as such is used as primary evidence under Section 62 of the Evidence Act, the same is admissible in evidence, without compliance with the conditions in Section 65-B of the Evidence Act" is to be read without the words "under Section 62 of the Evidence Act*". (*Para 32*)

- The Court observed that due to *non-obstante* language of Section 65B(1) this provision overrides any other provision thereby making it clear that when it comes to information contained in an electronic record, admissibility and proof thereof must follow the drill of Section 65B, which is a special provision in this behalf. The conditions under Sections 65B(2) and 65B(4) must be satisfied cumulatively. Sections 62 and 65 are irrelevant for this purpose. (*Para 22, 31*)

- However, the requirement under Section 65B(4) is unnecessary if the original document itself is produced. Where the computer happens to be on a system or network and it is impossible to physically bring such system or network to court, then the only means of providing information contained in such electronic record is in accordance with Section 65B(1), together with the requisite certificate under Section 65B(4). (*Para 32*)

- Where the requisite certificate has been sought from the person or the authority concerned, and the person or the authority concerned refuses to give such a certificate, or does not reply to such demand, the party asking for such certificate can apply to the court for its production under the provisions of the Evidence Act, CPC and/or CrPC. Once such an

application is made to the court, and the court orders or directs that the requisite certificate be produced by the person to whom it sends summons in this regard, the party asking for the certificate has done all that he can possibly do to obtain the requisite certificate. (*Para 45*)

- The Court observed that Section 65B does not speak of the stage at which such a certificate must be furnished to the court. In cases where either a defective certificate is given, or where such certificate has been demanded and is not given by the concerned person, the court must summon the person referred to in Section 65B(4) and require that the certificate be given by such person. In criminal cases, the requisite certificate can be directed to be produced by the court at any stage, as long as the trial is not over. (*Para 50*)
- Given that the certificate under Section 65B(4) may be given long after the electronic record has actually been produced by the computer, it is sufficient that the certificate is either to the best of the issuer's knowledge or belief. (*Para 58*)

4.4 INTERPRETATION OF SECTION 63(4) OF THE BHARATIYA SAKSHYA ADHINIYAM (BSA) IN COMPARISON TO SECTION 65B(4) OF THE INDIAN EVIDENCE ACT (IEA) REGARDING THE CERTIFICATION OF ELECTRONIC RECORDS:

The necessity of certification of electronic evidence as mandated in Section 65B(4), IEA is now placed in Section 63(4) of BSA. However, there are some glaring changes in Section 63(4), BSA vis-à-vis Section 65B(4), IEA. An analysis of those changes is vital for investigating officers as well as court and prosecutors. The changes are juxtaposed in a tabular form mentioned below:

Indian Evidence Act	**Bharatiya Sakshya Adhiniyam**
Section 65B: *(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say, ––* *(a) xxx* *(b) xxx* *(c) xxx* *and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.*	**Section 63:** *(4) In any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things shall be submitted along with the electronic record at each instance where it is being submitted for admission, namely: —* *(a) xxx* *(b) xxx* *(c) xxx* *and purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate) and an expert shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it in the certificate specified in the Schedule.*

**** Changes and emphasis highlighted***

As is conspicuous from the above table, earlier under Section 65B(4) of IEA, the admissibility of electronic records required a certificate issued by "*a person occupying a responsible official position concerning the operation of the relevant device or the management of the relevant activities*". However, the enactment of Section 63 of the BSA, seems to have introduced a more stringent and structured framework for certifying electronic evidence as the mandate of Section 63(4), BSA now prescribes that the certificate should be signed by *"a person in charge of the computer or communication device"*. It is expected that there will be interpretation of this new change by the Constitutional Courts of India.

On analyzing these two provisions it can be noted that the fundamental requirements for certification under Section 63 of the BSA remain unchanged in comparison to those under Section 65B(4) of the IEA. However, the BSA additionally requires the certificate to be also signed by an expert, in addition to the person in charge of the device concerned. A bare reading of Section 63(4), BSA shows that there is now requirement of a dual certification mechanism- one by an expert and the other by the person in charge or the management. It is also worth to mention that only for this purpose of dual certification, a Schedule has been inserted in Bharatiya Sakshya Adhiniyam which is also structured in two parts – Part A: Certificate to be filled by the Party; Part B: Certificate to be filled by the Expert.

This requirement of dual certification is apparently more stringent since now it is a mandatory that there has to be certification of an expert which was earlier not there in IEA. Introduction of this new mandate (Certification of an Expert) raises a question i.e., **who will be deemed to be an expert for the purpose of Section 63(4), BSA read with Schedule, IEA?**

In order to understand who can be an expert in context of Section 63(4) r/w Schedule (Part B), a combined reading of Section 39 (2) of BSA along with its explanation and Section 79A of IT Act show that such an expert would be *apparently "examiner of electronic evidence"*, notified by Central Government in the Official Gazette. Under Section 79A, IT Act any department, body or agency of Central Government or State Government can be an examiner of electronic evidence i.e., the expert for the purpose of Section 63 r/w Schedule, BSA. In compliance of Section 79A, IT Act, Central Govenrment has notified several departments as the Examiner of Electronic Evidence, which include:

1. Regional Forensic Science Laboratory (RFSL), Surat, Gujarat.[37]
2. Cyber Forensics & Digital Evidence Examiners Laboratory (CF&DEEL), Kolkata, West Bengal.[38]

37 [Noti. No. S.O. 3540(E)], dated August 3, 2023

38 [Noti. No. S.O. 3541(E)] Dated August 3, 2023

3. Forensics Science Department, 30A, Kamarajar Salai, Maylapre Chennai – 600004, Tamil Nadu.[39]

4. Cyber Forensics Laboratory, Navy Cyber Group, Naval Hqs, Ministry of Defence (Navy), 4th Floor Chanakya Bhawan, Chanakyapuri, New Delhi.[40]

5. Cyber Forensic Laboratory, Indian Computer Emergency, Response Team (CERT-In), Electronics Niketan, 6 CGO Complex, Lodhi Road, New Delhi.[41]

6. Cyber Forensic Laboratory, Army Cyber Group, DGIS (Directorate General of Information Systems) Enclave, Shankar Vihar New Delhi.[42]

However, it is pertinent to note that no body or agency of the Jharkhand Government has been notified as an Examiner of Electronic Evidence by the Central Government.

A crucial legal issue that arises is whether a report from a laboratory or organization that is not notified under Section 79A of the IT Act is admissible under Section 45A of the Indian Evidence Act (IEA), 1872, and Section 39(2) of the BSA, 2023. This issue was addressed in ***Shyam Sunder Prasad v. Central Bureau of Investigation***, wherein the court held[43]:

"The court held that Section 79A of IT Act, 2000 or Section 45 of IEA, 1872 do not provide that in absence of a notification in respect of a laboratory, opinion based on scientific examination given by a person well versed or skilled in such science, is not admissible in evidence. Unless such a bar is specifically provided in law, it cannot be read as an extension of Section 79A of the Information Technology Act that the report given by any other body/laboratory shall not be inadmissible in evidence in absence of notification. If the body/laboratory is notified, the authenticity of the report of such a body/laboratory may not be available for questioning".

The Court also highlighted Section 136 of IEA, 1872 that gives power to the court to decide admissibility of the evidence. Whether evidence is admissible or not, would depend on it being proved in accordance with law.

Since, there are only a handful of organizations that have been designated as Examiners of Electronic Evidence, the judgment is significant. Hence, if an evidence is prima facie declared inadmissible because the organization providing it is not notified by the Central Government, then it would add additional burden on the other states which do not have any such organization. Thus, it is on the Court to decide during cross-examinations and arguments as to whether the

39 [Noti. No. S.O. 5188(E)], dated November 27, 2024

40 [Noti. No. S.O. 5190(E)] Dated November 27, 2024

41 [Noti. No. S.O. 5191(E)] Dated November 27, 2024

42 [Noti. No. S.O. 5189(E)] Dated November 27, 2024

43 2022 SCC Online All 1790

report is admissible or not if it is given by a body which is well versed in science but not notified by Central govt.

Furthermore, Section 39(1) of the BSA (corresponding to Section 45 of the IEA) incorporates a significant change by inserting the residuary phrase *"any other field"* thereby making the opinion of an expert of any other field, including but not limited to experts in the fields of emerging technologies and the Information Technology, relevant in judicial proceedings. In contrast to the previous Section 45 of the IEA, which was exhaustive in specifying the fields from which experts could be called to testify before the trial court, Section 39(1) of the BSA adopts a more inclusive approach.

Another important point to be analysed is that earlier Section 65B(4), IEA used the phrase *"a person occupying a responsible official position*" with regard to the electronic device, whereas Section 63(4), BSA uses the term "*a person in charge*". A bare reading of the new phrase *"a person in charge*" of electronic device indicate that there is a probable legislative intent that the certification (for Part A of the Schedule) has to be specifically from a person in charge. As far as any private individual is concerned there may not be any ambiguity since to ascertain the scope of *"a person in charge,"* reference may be made to the Schedule of the BSA, which suggests that such an individual must have either ownership, maintenance, management, or operational control over the digital record in question. However, ambiguity may arise in interpretation of the term *"a person in charge"* of the computer or communication device when certificate is required from any government department. It is so because the mandate of law indicates that such government department now may be required to notify as to who would be the person in charge of the computer or communication device with regard to which Part A of the Schedule which would be required to be filled in.

HASH VALUE:

It is important for all the stakeholders i.e., Investigating Officers, Lawyers and Courts to have an understanding of hash value. It is so because now for the certificate for electronic evidence, it is mandatory to state the hash value of the electronic or digital record as well as to enclose the hash report. For understanding of "Hash Value" and "Hash Report" the readers may refer to Chapter 3 of this material.

4.5 COMPARATIVE CHART OF SECTION 65B (3) & (5) (IEA) AND SECTION 63 (3) & (5) (BSA):-

In Section 63 of the newly inacted Bhartiya Shakshya Adhiniyam, the terminology about nature of electronic devices has been expanded to include '*semiconductor memory*' and '*communication device*', which was earlier not there in Section 65 of the Indian Evidence Act. In subsection (3), the term "*computer*" has been replaced with "by means of one or more computers or communication devices," and new clauses (a) to (e) have been incorporated to provide a more comprehensive definition of computer.

Subsection (4) sees the phrase "*that is to say*" replaced with "*shall be submitted along with the electronic record at each instance……,*". The new insertion emphasizes that the certificate is a mandatory requirement and must accompany the electronic record at each instance it is presented as evidence. This ensures procedural clarity, removing any ambiguity regarding when the certificate needs to be submitted. Additionally, clause (b) now includes the words "or a communication device referred to in clauses (a) to (e) of sub-section (3)," expanding its applicability.

Clause (c) has been modified by replacing "*person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities*" with "*person in charge of the computer or communication device or the management of the relevant activities,*" clarifying the responsibility for issuing the certificate. Further, the words "and an expert" and "in the certificate specified in the schedule" have been added, reinforcing the authentication process. (Readers may refer to page number 82)

Moreover, clause (b) of subsection (5) of Section 63(5) of the Indian Evidence Act has been deleted, and the former clause (c) now corresponds to (b), incorporating the terms "*communication device*" and "*or by other electronic means as referred to in clauses (a) to (e) of sub-section (3),*" thereby ensuring consistency in terminology and applicability. This analysis critically examines the changes introduced in the new provision, particularly in Clause (3) and Clause (5), assessing their impact on the evidentiary value of electronic records.

Clause (3):

The primary distinction between the amended Section 63(3) of BSA and Section 65-B(3) of IEA lies in the expanded scope of '*electronic records*' and the inclusion of communication devices in Section 63(3). While both sections address the admissibility of electronic records and the treatment of multiple computing systems as a single unit, Section 63(3) explicitly incorporates '*communication devices*' alongside computers, recognizing their role in creating, storing,

and processing information. This shows that there is an adaptation to modern technological advancements where communication devices, such as Smartphone's and other networked devices, play a crucial role in digital record- keeping.

Aspect	Section 65B(3) - IEA, 1872	Section 63(3) - BSA, 2023	Changes/Observations
Scope of Function	Storing or processing information.	Creating, storing, or processing information.	Addition of "creating" broadens the scope of electronic record admissibility.
Terminology	Only refers to "computers."	Expands to "computers or communication device."	Recognizes modern digital devices beyond traditional computers.
Modes of Operation	(a) Combination of computers. (b) Different computers in succession. (c) Different combinations of computers in succession. (d) Any other manner involving successive operation.	(a) Standalone mode. (b) Computer system. (c) Computer network. (d) Computer resource enabling creation, processing, and storage. (e) Through an intermediary.	More detailed categorization in BSA, acknowledging networks, intermediaries, and evolving technology.
Treatment of Multiple Devices	All computers used during the period shall be treated as a single computer.	All computers or communication devices used during the period shall be treated as a single computer or communication device.	Inclusion of "communication device" ensures broader interpretation for digital evidence.

Clause (5)

Similar to the previous clause, the difference between Section 63 of the BSA, Clause (5), and Section 65B of the IEA, Clause (5), lies in the broader inclusion of 'communication devices' in Section 63 of the BSA, along with structural modifications and the omission of certain provisions present in Section 65B of the IEA.

Provision	Indian Evidence Act, 1872 (Section 65-B(3))	Bhartiya Sakshya Adhiniyam, 2023 (Section 63(3))	Observation/Comment
General Rule	Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—	Where over any period, the function of creating, storing, or processing information for the purposes of any activity regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by means of one or more computers or communication device, whether—	BSA expands the scope by including "**creating**" information, not just storing or processing. Additionally, "**communication device**" is introduced.
(a)	By a combination of computers operating over that period;	In standalone mode;	IEA focuses on multiple computers working together, while BSA starts with a **standalone mode**, broadening the scope.
(b)	By different computers operating in succession over that period;	On a computer system;	IEA emphasizes succession of different computers, whereas BSA includes **computer systems** as a broader concept.
(c)	By different combinations of computers operating in succession over that period;	On a computer network;	BSA includes **computer networks**, aligning with modern digital infrastructures, whereas IEA focuses only on successive operations.

Provision	Indian Evidence Act, 1872 (Section 65-B(3))	Bhartiya Sakshya Adhiniyam, 2023 (Section 63(3))	Observation/Comment
(d)	In any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers;	On a computer resource enabling information creation or providing information processing and storage;	BSA includes **computer resources**, further expanding the definition beyond simple succession of operations.
(e)	(Not present in IEA provision)	Through an intermediary;	BSA introduces intermediaries, covering scenarios where data is processed via third-party digital platforms or cloud computing.
	All the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.	All the computers or communication devices used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer or communication device; and references in this section to a computer or communication device shall be construed accordingly.	BSA extends the definition by explicitly including communication devices as part of a unified computing system.

Chapter 5: Bail and Compounding of Offences under IT Act, 2000

OFFENCES UNDER IT ACT: WHETHER BAILABLE OR NON-BAILABLE:

The classification of offences under the Information Technology Act (IT Act) as bailable or non-bailable is a critical issue, considering that the IT Act is a special Act. Section 77B of the IT Act explicitly provides that offences punishable with imprisonment of three years shall be bailable. However, the Act is silent about the offences punishable with more than three years. Although, Section 77B is an overriding provision which states that CrPC does not apply to this provision, a bare reading of Section 77B stipulates that it only applies to the offences punishable with imprisonment of three years. Therefore, reference mat be made to The First Schedule- "Part II-Classification of Offences Against Other Laws" of CrPC or BNSS for ascertaining as to whether offences punishable with imprisonment for more than 3 years are bailable or not. The first two rows of Part II of the First Schedule makes it clear that if the offence is punishable with imprisonment for 3 years and upwards but not more than 7 years or with death, imprisonment for life, or imprisonment for more than 7 years, such offence will be considered as non-bailable.

COMPOUNDING OF OFFENCES UNDER IT ACT:

Section 77A of IT Act, provides for compounding of offences by a court of competent jurisdiction, subject to the conditions that offences prescribing following punishment would be non-compoundable:

i. Imprisonment for a term exceeding three years,
ii. Life imprisonment,
iii. Cases of enhanced punishment due to previous conviction,
iv. Offences which effect socio-economic conditions of the country,
v. Offences committed against child below 18 years and
vi. Offences committed against women.

Sub-Section 2 to Section 77A gives opportunity to the person accused of an offence under this Act to file an application for compounding in the court in which offence is pending for trial and the provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 shall apply.

Bailable and Non- bailable offences and compounding of offences under IT Act, 2000 in tabular form:

Section of IT Act, 2000	Punishment	Bailable or Non-Bailable	Compoundable or Non-Compoundable
Section 65. Tampering with computer source documents	Imprisonment up to 3 years or with fine up to Rs. 2 lakh or with both	Bailable under IT Act	Compoundable
Section 66. Computer related offences	Imprisonment up to 3 years or with fine up to Rs. 5 lakh or with both	Bailable under IT Act	Compoundable
Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years or with fine up to Rs. 1 lakh or with both	Bailable under IT Act	Compoundable
Section 66C. Punishment for identity theft	Imprisonment of either description up to 3 years with fine up to Rs. 1 lakh	Bailable under IT Act	Compoundable
Section 66D. Punishment for cheating by personation by using computer resource.	Imprisonment of either description up to 3 years with fine up to Rs. 1 lakh	Bailable under IT Act	Compoundable
Section 66E. Punishment for violation of privacy.	Imprisonment up to 3 years or with fine up to Rs. 2 lakh or with both	Bailable under IT Act	Compoundable
Section 66F. Punishment for cyber terrorism.	Imprisonment up to imprisonment for life	Non-Bailable	Non-Compoundable

Section 67. Punishment for publishing or transmitting obscene material in electronic form.	*First Conviction:* Imprisonment of either description up to 3 years with fine up to Rs. 5 lakh	Bailable under IT Act	Compoundable
	Second or Subsequent conviction: Imprisonment of either description up to 5 years with fine up to Rs. 10 lakh	Non-Bailable	Non-Compoundable
Section 67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.	*First Conviction:* Imprisonment of either description up to 5 years with fine up to Rs. 10 lakh	Non-Bailable	Non-Compoundable
	Second or Subsequent conviction: Imprisonment of either description up to 7 years with fine up to Rs. 10 lakh	Non-Bailable	Non-Compoundable
Section 67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.	*First Conviction:* Imprisonment of either description up to 5 years with fine up to Rs. 10 lakh	Non-Bailable	Non-Compoundable
	Second or Subsequent conviction: Imprisonment of either description up to 7 years with fine up to Rs. 10 lakh	Non-Bailable	Non-Compoundable
Section 67C. Preservation and retention of information by intermediaries.	*Intentionally or knowingly contravenes the provision:* Imprisonment up to 3 years with fine	Bailable under IT Act	Compoundable
Section 68. Power of Controller to give directions	*Intentionally or knowingly fails to comply with any order:* Imprisonment up to 2 years or with fine up to Rs. 1 lakh or with both	Bailable under IT Act	Compoundable

Section 69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource	*Subscriber or intermediary or any person fails to assist the agency:* Imprisonment up to 7 years with fine	Non-Bailable	Non-Compoundable
Section 69A. Power to issue directions for blocking for public access of any information through any computer resource.	*Intermediary fails to comply with direction:* Imprisonment up to 7 years with fine	Non-Bailable	Non-Compoundable
Section 69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.	*Intermediary intentionally or knowingly contravenes the provisions:* Imprisonment up to 3 years with fine	Bailable under IT Act	Compoundable
Section 70. Protected system	*Securing or attempting to secure access to a protected system:* Imprisonment of either description up to 10 years with fine	Non-Bailable	Non-Compoundable
Section 70B. Indian Computer Emergency Response Team to serve as national agency for incident response.	*Service provider, intermediaries, data centres, body corporate or person fails to provide the information called for or comply with the direction:* Imprisonment up to 1 year or with fine up to Rs. 1 lakh or with both	Bailable under IT Act	Compoundable

Section 71. Penalty for misrepresentation.	Imprisonment up to 2 year or with fine up to Rs. 1 lakh or with both	Bailable under IT Act	Compoundable
Section 72. Penalty for Breach of confidentiality and privacy.	Imprisonment up to 2 year or with fine up to Rs. 1 lakh or with both	Bailable under IT Act	Compoundable
Section 72A. Punishment for disclosure of information in breach of lawful contract.	Imprisonment up to 3 year or with fine up to Rs. 5 lakh or with both	Bailable under IT Act	Compoundable
Section 73. Penalty for publishing electronic signature Certificate false in certain particulars.	Imprisonment up to 2 year or with fine up to Rs. 1 lakh or with both	Bailable under IT Act	Compoundable
Section 74. Publication for fraudulent purpose.	Imprisonment up to 2 year or with fine up to Rs. 1 lakh or with both	Bailable under IT Act	Compoundable

APPLICABILITY OF *SATENDER KUMAR ANTIL*, IN BAIL AND ARREST IN OFFENCES UNDER INFORMATION TECHNOLOGY ACT, 2000

Section 80[44] of the Information Technology Act, 2000, empowers the Police Officer of the rank of Inspector or above or any other officer of the Central Government or a State Government authorised by the Central Government to enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under the IT Act. At the same time, Section 80(3) of the Information Technology Act, 2000, mentions that the provisions of the Code of Criminal Procedure, 1973 (2 of 1974) shall, subject to the provisions of Section 80 of IT Act, apply, so far as may be, in relation to any entry, search or arrest, made under the section.

The Supreme Court in the case of ***Satender Kumar Antil v. CBI,* (2022) 10 SCC 51**, held that any arrest made in a cognizable offence for which the punishment is less than seven years with or without fine must be subject to Section 41[45] of CrPC, which says that an arrest could only

44 **80. Power of police officer and other officers to enter, search, etc.**—(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a [Inspector], or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

Explanation.—For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 (2 of 1974) shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

45 **41. When police may arrest without warrant.**—(1) Any police officer may without an order from a Magistrate and without a warrant, arrest any person—

[(*a*) who commits, in the presence of a police officer, a cognizable offence;

(*b*) against whom a reasonable complaint has been made, or credible information has been received, or a reasonable suspicion exists that he has committed a cognizable offence punishable with imprisonment for a term which may be less than seven years or which may extend to seven years whether with or without fine, if the following conditions are satisfied, namely:—

(i) the police officer has reason to believe on the basis of such complaint, information, or suspicion that such person has committed the said offence;

(ii) the police office is satisfied that such arrest is necessary—

(*a*) to prevent such person from committing any further offence; or

(*b*) for proper investigation of the offence; or

(*c*) to prevent such person from causing the evidence of the offence to disappear or tampering with such evidence in any manner; or

(*d*) to prevent such person from making any inducement, threat or promise to any person acquainted with the facts of the case so as to dissuade him from disclosing such facts to the Court or to the police officer; or

(*e*) as unless such person is arrested, his presence in the Court whenever required cannot be ensured,

follow when the officer is satisfied that there is a reason to believe or suspect, that the said person has committed an offence, and there is a necessity for an arrest – to prevent the committing of any further offence, proper investigation, and to prevent him/her from either disappearing or tampering with the evidence, and when his/her presence is required after arrest for production before the court and the same cannot be assured. The police officer is duty bound to record in writing the reasons for making or not making an arrest, except in cases where the alleged offense exceeds seven years, among other reasons. And any non-compliance would entitle the accused to a grant of bail. (Para 23 – 25)

The Supreme Court in light of the judgment in ***Arnesh Kumar v. State of Bihar*** **(2014) 8 SCC 273 (Para 7 - 12)**, directed all the State Governments and the Union Territories to comply with the mandate of Section 41-A. The Supreme Court gave a reason that this would certainly take care of not only the unwarranted arrests, but also the clogging of bail applications before various courts as they may not even be required for the offences up to seven years.

---

and the police officer shall record while making such arrest, his reasons in writing.

[Provided that a police officer shall, in all cases where the arrest of a person is not required under the provisions of this sub-section, record the reasons in writing for not making the arrest.]

(ba) against whom credible information has been received that he has committed a cognizable offence punishable with imprisonment for a term which may extend to more than seven years whether with or without fine or with death sentence and the police officer has reason to believe on the basis of that information that such person has committed the said offence;]

(c) who has been proclaimed as an offender either under this Code or by order of the State Government; or

(d) in whose possession anything is found which may reasonably be suspected to be stolen property and who may reasonably be suspected of having committed an offence with reference to such thing; or

(e) who obstructs a police officer while in the execution of his duty, or who has escaped, or attempts to escape, from lawful custody; or

(f) who is reasonably suspected of being a deserter from any of the Armed Forces of the Union; or

(g) who has been concerned in, or against whom a reasonable complaint has been made, or credible information has been received, or a reasonable suspicion exists, of his having been concerned in, any act committed at any place out of India which, if committed in India, would have been punishable as an offence, and for which he is, under any law relating to extradition, or otherwise, liable to be apprehended or detained in custody in India; or

(h) who, being a released convict, commits a breach of any rule made under sub-section (5) of Section 356; or

(i) for whose arrest any requisition, whether written or oral, has been received from another police officer, provided that the requisition specifies the person to be arrested and the offence or other cause for which the arrest is to be made and it appears therefrom that the person might lawfully be arrested without a warrant by the officer who issued the requisition.

Corresponding Law: S. 54 of Act V of 1898.

[(2) Subject to the provisions of Section 42, no person concerned in a non-cognizable offence or against whom a complaint has been made or credible information has been received or reasonable suspicion exists of his having so concerned, shall be arrested except under a warrant or order of a Magistrate.]

Corresponding Law: S. 55 of Act V of 1898.

Also, in ***Satender Kumar Antil v. CBI,*** **(2022) 10 SCC 51,** the Supreme Court categorized offenses into different types (A, B, C, and D) based on their severity and prescribed a framework for granting bail, emphasizing the importance of personal liberty and reducing unnecessary arrests.

Categories/Types of Offences

(A) Offences punishable with imprisonment of 7 years or less not falling in Categories B & D.

(B) Offences punishable with death, imprisonment for life, or imprisonment for more than 7 years.

(C) Offences punishable under Special Acts containing stringent provisions for bail like NDPS (Section 37), PMLA (Section 45), UAPA [Section 43-D(5)], Companies Act, [Section 212(6)], etc.

(D) Economic offences not covered by Special Acts.

In **Category A** offences, after the filing of the charge-sheet or complaint and taking cognizance, an ordinary summons is issued at the first instance, including permitting appearance through a lawyer. If the accused does not appear despite the service of summons, a bailable warrant for physical appearance may be issued. If the accused still fails to appear despite the issuance of a bailable warrant, a Non-Bailable Warrant (NBW) may be issued. However, the NBW may be cancelled or converted into a bailable warrant or summons without insisting on the physical appearance of the accused if an application is moved on behalf of the accused before the execution of the NBW, along with an undertaking to appear physically on the next date(s) of hearing. When such an accused appears, their bail application may be decided without taking them into physical custody or by granting interim bail until the bail application is decided.

In **Category B and D** offences, upon the appearance of the accused in court pursuant to the process issued, the bail application is to be decided on merits.

In **Category C** offences, the bail application is to be decided on merits upon the appearance of the accused in court pursuant to the process issued, similar to Categories B and D. However, an additional condition applies, requiring compliance with the specific bail provisions under special laws such as Section 37 of the NDPS Act, Section 45 of the PMLA, Section 212(6) of the Companies Act, Section 43-D(5) of the UAPA, and POSCO, among others.

So, **Yes,** the guidelines laid down in ***Satender Kumar Antil v. CBI,*** **(2022) 10 SCC 51,** regarding bail principles are applicable to offenses under the Information Technology (IT) Act as well. For IT Act cases, whether the guidelines apply depends on the classification of the offense:

1. Category A – Offenses punishable with up to 7 years (e.g., Section 66 of the IT Act for hacking or identity theft). Bail should generally be granted at the police or Magistrate's level.

2. Category B & C – More serious offenses involving economic offenses or special acts, which may require judicial discretion but still emphasize bail as a norm unless special circumstances exist.

3. Category D – Heinous offenses requiring strict scrutiny (not commonly relevant for IT Act cases).

The guideline laid down by the Supreme Court in the case of ***Satender Kumar Antil v. CBI,*** **(2022) 10 SCC 5,** will be applicable to offences committed under the Information Technology (IT) Act, 2000, unless the offense under the IT Act is particularly grave, the case will guide bail decisions, favoring release over prolonged custody unless specific factors justify otherwise.

The IT Act does not explicitly exclude the application of Section 41 CrPC or the principles elucidated in *Satender Kumar Antil*, making them applicable to IT Act offenses. Therefore, the *Satender Kumar Antil* guidelines, which are based on the CrPC, apply to arrests and bail considerations under the IT Act, subject to the specific provisions of the IT Act itself.

However, when dealing with certain severe offenses, such as cyber terrorism or those involving child sexual abuse material (CSAM), the court must be exceptionally cautious when considering bail. These offenses include publishing or transmitting in electronic form any material containing a sexually explicit act or conduct, particularly depictions of children engaged in such acts; creating text or digital images, collecting, seeking, browsing, downloading, advertising, promoting, exchanging, or distributing material in any electronic form depicting children in an obscene, indecent, or sexually explicit manner; cultivating, enticing, or inducing children into online relationships with one or more children for sexually explicit acts or in a manner that may offend a reasonable adult using a computer resource; facilitating the online abuse of children; and recording in any electronic form one's own abuse or that of others pertaining to sexually explicit acts with children, etc. In these cases, the court must carefully weigh the potential risks to the community, and be cautious in granting bails.

ARTICLES

CSassy Tales – Cybercrime Stories & The Law©[47] – Excerpts

- N. S. Nappinai, Senior Advocate, Supreme Court of India

Law is at a nascent stage with respect to cybercrime, whilst the cybercriminal is an evolved species. The primary challenge to combating cybercrimes is not only lack of sufficient enactments even against existing trends of crimes but also enforcement.

(Nappinai N. S (2017)[48])

Crime pays and cybercrimes pays better – or so the criminals appear to have surmised and the exponential spurt in cybercrimes appears to support this assumption. It therefore falls to the realm of law and legal systems to prove the cybercriminal wrong by ensuring that the laws of the land are better enforced whilst we await further or possibly better laws.

The Book, "CSassy Tales – Cybercrime Stories & The Law"[48], was authored by Ms. N. S. Nappinai to capture the legal minefield of cybercrimes and protective and preventive measures against them and critically, how existing laws may be applied to combat these evolving crimes. The book uses storytelling as a methodology to pass on the message of cyber hygiene and cyber safety. Significantly it also addresses the pressing need for creating awareness on the fine line between pranks or jokes and crimes to ensure deterrence against, particularly children or young adults committing crimes inadvertently.

The excerpts extracted hereunder provide the reader with a teaser of what they may expect from the book and also helps understand the evolving face of cybercrimes. It also demystifies cyber colloquialisms such as "catfishing", "griefing" or "revenge porn" and explains how the crimes are still covered under existing provisions.

Cybercrimes:

Offences such as cyber-bullying, cyber stalking, cyber frauds or scams abound from early days of adaptation to digital domains. Defacement of websites, hacking, virus attacks, denial of

47 Nappinai. N. S. (2022). CSassy Tales – Cybercrime Stories & The Law. Oakbridge Publishing

48 Available at: https://www.amazon.in/CSassy-Tales-Cybercrime-Stories-Law/dp/9391032214;

service attacks were norms even before our Information Technology Act, 2000 (as amended) ("IT Act") was enacted. Yet several violations, which amount to crimes such as hacking, virus attacks, denial of service attacks or defacements through deleting, destroying or altering digital data were listed as a civil offence under S.43 of the IT Act 2000. Through reading in Section 66 IT Act, as amended to make dishonest and fraudulent acts under Section 43 IT Act a criminal offence, this lacunae was plugged.

Use of colloquial slang to describe evolving cybercrimes further complicates enforcement, as there is misapprehension not only in the minds of victims but also enforcers that such acts may not be crimes.

Illustrations are, as under:

CSassy Tales: Excerpts:

Chapter I (B) of the Book: Griefing & Support Group Systems For Educational Institutions

FICTION

X was at the college support group gathering. To say it was an eye-opener was an understatement.

'Griefing' – not a word most are used to and it is but natural to assume that someone just made an English faux pas! When X heard of griefing first, she, as many assumed that it was about grieving. It was both surprising and in a strangely twisted way heartening for her to meet other victims of online gaming abuse. Learning that 'griefing' or the acts of willfully abusing and provoking anger in online gaming; ganging up by many players against one player to stop the victim from progressing in a game or as in her case even assaulting online were emerging threats in online gaming. X realised many gamers had been 'griefed' at least once, if not more, especially when players think that attacking and succeeding against one player is not likely to succeed one-on-one.

…

CSASSY'S REALITY BITES

Virtual rape is not new. In 1993, which seems like a different era, Julian Dibbell wrote about 'A Rape in Cyberspace'. The incident refers to an online character Mr. Bungle or more precisely its creator using a malware 'Voodoo Doll' to control other characters to perform actions they did not intend to. The scene was a virtual living room on a virtual platform LAMBDAMOO, which was a virtual world in the form of a rustic mansion. LAMBDAMOO was a MUD or Multi-User Dimension, which refers to virtual platforms allowing multiple virtual characters to interact in virtual surroundings. The virtual reality experience turned into a horrific experience for the

participants, who were manipulated by Mr. Bungle to perform sexual acts and then self-harm, including violent actions against themselves or to be more precise their virtual selves.

…

Take the instance of a mom-gamer on the Metaverse who reports a gang rape on the Metaverse in February 2022. The 43-year-old reports virtual sexual abuse and gang rape by 3-4 male avatars, who ape the real-world modus of raping her avatar and also taking photos. This is akin to the Supreme Court case in Prajwala mentioned above[49]. In most cases of sexual abuse in recent times, as elaborated in the stories above, offenders believe that shaming the victims through recordings of the violent crimes against the victims and threatening to share online or with friends and family will ensure silence and inaction by victims. Unfortunately, this is often the case and such inaction merely emboldens criminals to commit more crimes against the same victims or against other victims. These are the reasons for ensuring that all such crimes offline or online are reported and action initiated against offenders.

…

Chapter I (C): Flaming, Dissing, Ghosting, Outed, Honey Traps, Catfishing – The New Cybercrime Dictionary

FICTION

Knowing of other victims was an important journey for X – not because she was looking for companions in misery but because her innate trait to help others in distress took over and dragged her out of her misery into action. Her quick mind started evaluating how important better awareness of such trending offences and violence online was important for her peers. She also realised that despite such an important support system being available on campus she was not even aware of it. Everyone should know about these issues was her first thought. An emotional outburst dragged her back to the shares in the group.

There was a veritable new dictionary emerging from online violence. Hate speech targeting women and children seemed common.

Abusers using 'flaming' which refers to trolls purposely ganging up and targeting the victim with a barrage of angry or "abusive online messages", intended to 'provoke the victim' for the sole purpose of perpetuating arguments and online "war of words". Victim 'B' spoke in the group about how she was targeted when she posted online during the #Metoo movement. B believed that she was 'flamed'

49 The Supreme Court of India took suo motu action by registering a letter received about failure to takedown such content in Re: *Prajwala Letter dated 18.2.2015. Violent Videos & Recommendations* and passed a seminal order in October 2017, [(2018) 15 SCC 551], to place preventive and protective measures for protection of women and children online.

either because of her gender or community or both. 'flaming' it seemed was often a 'hate crime' than just cybercrime or cyber-bullying.

…

CSassy's Pointers on Law & Remedies

…

Each story above indicates the increasing threats of cybercrimes against students. New phraseology is emerging with each crime. The modus, as also the remedies however are akin to old crimes and punishments therefor. Old and existing laws are still expected to deal with these new age crimes with the millennial names. Often the issue that most policymakers face is if the law is supposed to encompass each such evolving crime through specific provisions carrying the same names used colloquially. This is neither feasible nor advisable. This assumption also leads one to believe there are no remedies in law against such evolving crimes. This is incorrect and misleading. The heading or caption in a legal provision is irrelevant for its interpretation. All that needs to be applied are existing laws to the facts of each case. The mode and manner in which a violent act or offence is committed will decide the provisions to be applied for prosecutions.

For the above fictional tales of honey traps, griefing, etc., some of the criminal provisions that could be evaluated, are, as under:

***Indian Penal Code, 1860:** Applicable Sections & Criminal Offences:*

- ***Section 153A** - Hate crime, as applicable*
- ***Section 384 to 387 -** Extortion, as applicable*
- ***Section 509** - Outraging Modesty of a woman*
- ***Section 354A** - Sexual Harassment, where applicable*
- ***Section 354C** - Voyeurism, where applicable*

Information Technology Act, 2000 (as amended): Applicable Sections & Criminal Offences

- ***Section 66C** - Identity theft*
- ***Section 66D** - Cheating by Personation*
- ***Section 66E** - Violation of Privacy*
- ***Section 67, 67A or 67B, as applicable** - Publishing or transmission of obscene or sexually explicit content or of child sexual abuse material/child pornography*

The Protection of Children From Sexual Offences Act, 2012 ("POCSO"): Applicable Sections & Criminal Offences:

Based on facts, ***Sections 11 to 14*** *may be applicable.*

There may be some instances such as violence in online gaming on the avatar, as opposed to the person, where existing laws may not be sufficient. In such instances and also in others, victims could seek remedies through theplatform or service providers.

Chapter 24: Cryptocurrency – An Unsafe Bet[50]

REALITY BEFORE FICTION

IPL was until recently all about cricket ... and yes, in some instances more about those faith-shattering betting scam allegations. It's not been so of late. After all, what better platform to use to promote a product (i.e., cryptocurrency) that appeals most to the young millennials? Cryptocurrency ads have overshadowed excitement from the cricket matches to intrigue and induce viewers to become first-time investors and risk-takers. It has also raised issues of the use of cryptocurrency for money laundering leading to informal curbs. None of which appear to have dented the recent spurt of enthusiasm for cryptocurrencies or what is now termed as 'crypto assets'.

Cryptocurrency ads are not limited to IPL matches. They are everywhere. Your coffee shop around the corner to even a food delivery service carrying that tiny flyer telling you how to invest in cryptocurrencies.

Most investors barely understand what is a 'cryptocurrency'. None even pause to think about accountability including who would they reach out to if their investments nose dive. The fine print is even finer for an audience that is well-primed to click without reading.

'Morris Coin" – Similar to the Fictional "X Coin" Story above

The Morris Coin Scam was structured around the concept of ICOs. Here was a coin that the promoters promoted through a multi-level marketing mode with tall claims that the value would soar in a short while. Ten coins were slotted at a value of Rs.15,000 with restrictions on trading for a period of 300 days. With the "Morris Coin" being listed with "a Coimbatore-based cryptocurrency exchange called Franc Exchange", investors' trust ran high along with their risk appetite. Ultimately, it is the lure of high returns that captures the risk-taker investors who are the targets for cryptocurrency investments. Stories of unimaginable wealth creation out of nothing that abound with respect to cryptocurrencies are used to bait investors into such possible scams. The COVID19 pandemic with its lockdowns, more digital time and loss of income, and need for quick returns push investors to fall for scams.

50 Visit www.cybersaathi.org for a more information on cryptocurrencies and the evolving legal / regulatory frameworks in India and other jurisdictions.

In January 2022, the Enforcement Directorate ("ED"), which is India's anti- money laundering law enforcement agency, reportedly broke this "Morris Coin" cryptocurrency scam that centred around Kerala. With investigations having just begun, we will have to wait and watch the outcome of this prosecution. However, that investors were deprived of money and cryptocurrency, which was in turn used to purchase immovable properties instead of applying it to launch "Morris Coin" and ensure returns to investors appears to be the crux of this case.

That this possible scam was conceptualised and launched by very young and ingenious criminals is cause for concern.

Ponzi Modus

Most crypto crimes use the Ponzi or Pyramid Scheme model. This helps to bait first-time investors and that too using their own friends and family to induce them. Most investors do not realise that their own money is just being circulated to induce more to join the ever-expanding pyramid. As with Ponzi schemes that target the greed of an investor through impossibly high returns, crypto scams also do the same.

The fictional tale is also reminiscent of the "Gainbitcoin case", which used the multi-level marketing process for promoting a scheme that promised to double cryptos through "mining" processes and encouraged investors to first purchase cryptos and then invest them with the entity. The promoters, as per the criminal prosecution initiated, had siphoned out several thousand rupees from investors through a Ponzi scheme to purchase expensive properties including in the Burj Khalifa.

…

It is not just cricket – football players are much sought-after influencers. Spanish Footballer Andres Iniesta and others were engaged by Binance, as per news reports, to promote the crypto exchange platform and Andres' Twitter posts immediately drew flak from the Spanish Regulator who asked him to read up on the risks involved[51]. With the new laws proposed for Spain, such tweets would carry the risks and liabilities attached.

CSassy's Pointers on Law & Remedies

You do have remedies against crypto frauds. Hence victims should ensure that they complain about crypto frauds. Remember your silence not only causes you loss but also helps the criminal to con many others. If you had spoken out; If you had filed that criminal complaint; probably millions would have been saved. Hence speak out. Share your stories and file that criminal complaint. Do not fear systems. Seek your remedies.

51 https://www.ft.com/content/64d4cfa6-e277-4a5b-a8b7-f7def5b82e00.

Further the Prize Chits and Money Circulation Schemes (Banning) Act, 1978 makes Ponzi or Pyramid schemes also illegal. Hence crypto frauds committed using such methods can also be prosecuted using the said law.

In the cases of fraud set out above, both IT Act and IPC provisions were applied. Further, each State also has an Investor protection law. For instance,Maharashtra has the Maharashtra Protection of Interest of Depositors (In Financial Establishments) Act, 1999 ("MPID" Act). Several of the scams set outabove have been booked under such special State laws also.

The applicable IT Act provisions, depending on whether the scam involved identity theft and impersonation for the purpose of cheating, would be Sections 66C & 66D of the IT Act.

Sections 419, 420 of the IPC are invoked in most of the above scam cases.

Further, as set out above, the Prize Chits and Money Circulation Schemes (Banning) Act, 1978, and also the various State Investor Protection laws are also used to prosecute the Indian scamsters.

All of the above gives some pointers on the remedies available to victimsof Crypto scams.

CSassy Tales: Excerpts Closed

Teaser Tales

The above are but a teaser to indicate the flow of contents of the book and are shared for the benefit of readers. The above excerpts themselves point to the methodology one could adapt in dealing with evolving cybercrimes. It explains how existing legal provisions may be invoked to help combat, what otherwise seems to be complex crimes. The purpose is to ensure that crimes do not go unpunished for want of clarity on applicability of existing provisions[52].

52 Please read the book CSassy Tales – Cybercrime Stories & The Law for a more detailed enunciation on both cybercrimes and also the legal provisions that may be invoked.

Regulation of Cyber Crimes Through Bharatiya Nyaya Sanhita – An Analysis

Dr. Nagarathna. A.[53]

INTRODUCTION:

Cyber-crime regulation has today become one of the important objectives of Criminal Justice Administration. Every legal system including Indian is framing and revising its laws to effectively curb cyber-crimes. Both substantive as well as procedural laws of India have undergone changes in this direction since last few years. The newly introduced criminal laws of India – Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita and Bharatiya Sakshya Adhiniyam have also undergone changes for the same reason. This article attempts to analyse the provisions of Bharatiya Nyaya Sanhita through which cyber-crimes can be regulated.

CYBER-CRIME REGULATION AND INDIAN CRIMINAL LAWS

Cyber-crimes of today are of various forms. They include offences committed with the latest form of cyber technology including Internet of Things, communication devices, smart gadgets, etc. Indian Information Technology Act of 2000 was amended in the year 2008 in order to expand its scope to include various forms of cyber-crimes such as – hacking, data theft, data destruction, online frauds, identity theft, cyber pornography, child pornography etc. On the other hand, conventional crimes such as defamation, cheating, fraud, etc which can be committed with the use of cyber technology continued to be regulated through the then Indian Penal Code. The Code underwent changes in the year 2013 with an object of more strictly regulating offences committed against women. This amendment led to insertion of provisions criminalising cyber stalking, online sexual harassment, voyeurism, etc. Further sharing of online hateful content or other abusive material too could be regulated through IPC. Apart from IT Act of 2000 and IPC, there are other special enactments such as Protection of Children from Sexual Offences Act of 2013, POSH Act, ITPA, etc which can also be extended to cyber-crime domain depending upon the nature of such crime.

53 Associate Professor of Law, National Law School of India University, Bengaluru. The author can be reached at nagarathna@nls.ac.in

BHARATIYA NYAYA SANHITA AND CYBER CRIMES

Bharatiya Nyaya Sanhita [henceforth referred to as BNS] being a new version of the Indian Substantive Criminal Law aims to redesign the law to suit the changed socio-economic scenario of the country. It also intends to make the criminal law wider to cover offences there were earlier not dealt with through IPC – such as terrorism, organised crime, etc. Some of the provisions are made gender-neutral in nature so as to protect victims of any gender.

THE FOLLOWING ARE SOME OF THE PROVISIONS OF BNS THAT CAN BE USED TO REGULATE CYBER-CRIMES:

OFFENCES AGAINST WOMEN:

There are certain forms of cyber-crimes considered as gender-specific for often been the ones targeting women. This includes cyber stalking, voyeurism, online harassment, etc. IPC through the amendments made in the year 2013 and then again in 2018 dealt with some of these offences. Today BNS too continues to deal with these offences as gender specific crimes. Some of such offences includes the following:

Voyeurism: Section 77 of BNS which replaces Section 354C of IPC regulates Voyeurism. While the IPC provision in this regard was limited in its scope since it only covered a 'man' as an offender BNS makes it wider to cover a person of any gender as it replaces the word 'man' with the words 'whoever.' According to Section 77: "Whoever watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, & shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than 3 years, but which may extend to 7 years, and shall also be liable to fine."

Words of gesture insulting modesty of woman: According to Section 79, BNS which replaces section 509 of IPC, "Whoever, intending to insult the modesty of any woman, utters any words, makes any sound or gesture, or exhibits any object **in any form**, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to three years, and also with fine." The words **'in any form'** being added through BNS makes the provision wider to cover offences covered through e-form or by way of using

cyber technology. For example, if a person shows any pornographic content that is e-form to a woman, he commits an offence under this provision. Similarly, if a person sends an abusive message through e-modes that has any content in form of word or sound and if such content is sent with an intent to insult modesty of a women, he can be booked under this provision.

Cyber Stalking: Stalking includes cyber stalking and thereby comes under the purview of Section 78 which replaces section 354D of IPC. This section did not undergo any change through BNS and continues to criminalise the offence of stalking if it is committed by a man against a woman[54].

Sexual Harassment: Though section 75 of BNS which replaces Section 354A[55] of IPC has not undergone any change, yet it covers the offence of online sexual harassment as it covers under its ambit offences of making advances with unwelcome and explicit sexual overtures, demanding or requesting sexual favours, showing pornography against the will of a woman and making sexually coloured remarks, which can be committed both in online as well as offline domain.

CRIMES AGAINST CHILDREN OR IN RELATION TO CHILDREN:

Though most of the cybercrimes committed against children such as child pornography, online grooming, online sexual harassment of child, etc are dealt with under the Protection of Children from Sexual Offences Act 2013, yet certain offences such as trafficking of children is covered under BNS. Further, BNS has introduced a new provision through which using a child to commit an offence is made punishable.

54 According to Section 78, BNS: "(1) Any man who— (i) follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or (ii)monitors the use by a woman of the internet, e-mail or any other form of electronic communication, commits the offence of stalking: Provided that such conduct shall not amount to stalking if the man who pursued it proves that— (i)it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or (ii) it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or (iii)in the particular circumstances such conduct was reasonable and justified. (2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine."

55 According to Section 765: "(1) A man committing any of the following acts: — (i)physical contact and advances involving unwelcome and explicit sexual overtures; or (ii)a demand or request for sexual favours; or (iii)showing pornography against the will of a woman; or (iv) making sexually coloured remarks, shall be guilty of the offence of sexual harassment. (2) Any man who commits the offence specified in clause (i) or clause (ii) or clause (iii) of sub-section (1) shall be punished with rigorous imprisonment for a term which may extend to three years, or with fine, or with both. (3) Any man who commits the offence specified in clause (iv) of sub-section (1) shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both."

According to Section 95, "Whoever hires, employs or engages any child to commit an offence shall be punished with imprisonment of either description which shall not be less than three years but which may extend to ten years, and with fine; and if the offence be committed shall also be punished with the punishment provided for that offence as if the offence has been committed by such person himself." This section is wide enough to cover offences of child pornography for the commission of which a chid is used or exploited. According to the statutory explanation provided under this provision, "Hiring, employing, engaging or using a child for sexual exploitation or pornography is covered within the meaning of this section."

OFFENCES AGAINST STATE:

Today online platforms are used by criminals to commit offences that affects the interest of State. Some of such offences are dealt with under IT Act. Additionally, BNS too regulates certain offences that affects State's interest especially for being the one that affects integrity, security and sovereignty of State. Following are some of such provisions from BNS:

Cyber Terrorism:

While the Information Technology Act through Section 66F deals with Cyber terrorism, the offence can now also be dealt with through BNS. BNS has also bought under its ambit legal provision related to terrorism. Section 113 while defining terrorist act recognises terrorism committed by using "by any other means of whatever nature" thereby covering under its ambit means that can be adopted with the use of cyber technology. According to this provision if a person by using such means if causes or is likely to cause "(i) death of, or injury to, any person or persons; or (ii) loss of, or damage to, or destruction of, property; or (iii) disruption of any supplies or services essential to the life of the community in India or in any foreign country; or (iv) damage to, the monetary stability of India by way of production or smuggling or circulation of counterfeit Indian paper currency, coin or of any other material; or (v) damage or destruction of any property in India or in a foreign country used or intended to be used for the defence of India or in connection with any other purposes of the Government of India, any State Government or any of their agencies; .." commits terrorist act. This provision can be hence extended to acts of cyber terrorism such as cyber-attacks on critical information infrastructure, etc. Also using online mode to conspire, abet or advocate, advise or incite terrorist act[56] or organising any camps including on virtual platform to train or recruit a terrorist[57] are also made punishable offences under the Sanhita.

56 Section 113(3) of BNS

57 Section 113(4) of BNS

Other Offences against State:

Other offences against State such as waging war against State or conspiring to commit such offence, etc., are dealt with from section 147 to 158 of BNS. Since most of these offences can be committed on online platform, they also become relevant part cyber-crime regulatory framework. Most importantly the following provisions explicitly covers offences committed with the use of electronic communication mode thereby brining under its ambit certain forms of cyber-crimes:

- Section 152[58] which covers offence endangering sovereignty, unity and integrity of India covers offences committed through electronic communication. It is interesting to note that while the new law has deleted section 124A of IPC [which was dealing with sedition], this section – that is – section 152 of BNS is criticised for being a revised version of sedition. This provision in fact fills the gap created due to the striking down of Section 66A of the IT by Supreme Court through its decision in Shreya Singhal v. Union of India.[59]

- Section 192 which replaces Section153 of IPC covers offences of provoking riot. According to this provision: "Whoever malignantly, or wantonly by doing anything which is illegal, gives provocation to any person intending or knowing it to be likely that such provocation will cause the offence of rioting to be committed, shall, if the offence of rioting be committed in consequence of such provocation, be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both; and if the offence of rioting be not committed, with imprisonment of either description for a term which may extend to six months, or with fine, or with both."

- Section 196 which replaces Section 153A of IPC is revised as follows: "(1) Whoever—(a)by words, either spoken or written, or by signs or by visible representations or through electronic communication or otherwise, promotes or attempts to promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, disharmony or feelings of enmity, hatred or ill-will between different religious, racial, language or regional groups or castes or communities."[60] This provision

58 Section 152 BNS states: "Whoever, purposely or knowingly, by words, either spoken or written, or by signs, or by visible representation, or by electronic communication or by use of financial mean, or otherwise, excites or attempts to excite, secession or armed rebellion or subversive activities, or encourages feelings of separatist activities or endangers sovereignty or unity and integrity of India; or indulges in or commits any such act shall be punished with imprisonment for life or with imprisonment which may extend to seven years, and shall also be liable to fine."

59 AIR 2015 SC 1523

60 This provision continues to criminalise offences earlier covered under Section 153A by stating: "(b) commits any act which is prejudicial to the maintenance of harmony between different religious, racial, language or regional groups or castes or communities, and which disturbs or is likely to disturb the public tranquillity;

in fact is revised to expressly state that the provision can be used even if the said offence if is committed with the use of electronic communication. Hence sharing of any online hateful content or sharing of any e-content which can promote disharmony or enmity or heartedness or ill-will between people is criminalised under this provision.

- According to Section 197 which replaces Section 153B of IPC, using words – either spoken or written or making a signs or visible representations or using electronic communication modes or other modes and thereby making or publishing "any imputation that any class of persons cannot, by reason of their being members of any religious, racial, language or regional group or caste or community, bear true faith and allegiance to the Constitution of India as by law established or uphold the sovereignty and integrity of India"[61] commits an offence under this provision. The provision further covers offences of making an assertion, or counselling or advising or propagating or publishing "that any class of persons shall, by reason of their being members of any religious, racial, language or regional group or caste or community, be denied, or deprived of their rights as citizens of India."[62] Similarly making or publishing "any assertion, counsel, plea or appeal concerning the obligation of any class of persons, by reason of their being members of any religious, racial, language or regional group or caste or community, and such assertion, counsel, plea or appeal causes or is likely to cause disharmony or feelings of enmity or hatred or ill-will between such members and other persons" is an offence under this provision.[63]

- **False Information / Fake Information / Information Warfare:** In addition to these provisions being continued from IPC to BNS via Section 197 of BNS, the new Sanhita has added an additional provision that is clause (d) to Section 197 according to which making or publishing false or misleading information, jeopardising the sovereignty, unity and integrity or security of India is an offence.[64]

  This provision aims to deal with the menace of false information or fake information or information warfare which has become a serious concern today. Note that earlier the

or (c) organises any exercise, movement, drill or other similar activity intending that the participants in such activity shall use or be trained to use criminal force or violence or knowing it to be likely that the participants in such activity will use or be trained to use criminal force or violence, or participates in such activity intending to use or be trained to use criminal force or violence or knowing it to be likely that the participants in such activity will use or be trained to use criminal force or violence, against any religious, racial, language or regional group or caste or community and such activity for any reason whatsoever causes or is likely to cause fear or alarm or a feeling of insecurity amongst members of such religious, racial, language or regional group or caste or community,

61 Section 197 (1)(a) of BNS

62 Section 197 (1)(b) of BNS

63 Section 197 (1)(c) of BNS

64 Section 197 (1)(d) of BNS

offence of sharing of any false information could be regulated through Section 66A of the Information Technology Act, 2000. However, this provision was stuck down by the Supreme Court through its decision in Shreya Singhal v. Union of India[65].

- Further Section 353 of BNS which replaces Section 505 of IPC , making, publishing or circulating "any statement, false statement, rumour or report including through electronic means - (a) with intent to cause, or which is likely to cause, any officer, soldier, sailor or airman in the Army, Navy or Air Force of India to mutiny or otherwise disregard or fail in his duty as such; or (b) with intent to cause, or which is likely to cause, fear or alarm to the public, or to any section of the public whereby any person may be induced to commit an offence against the State or against the public tranquillity; or (c)with intent to incite, or which is likely to incite, any class or community of persons to commit any offence against any other class or community"[66] is an offence. Also "Whoever makes, publishes or circulates any statement or report containing false information, rumour or alarming news, including through electronic means, with intent to create or promote, or which is likely to create or promote, on grounds of religion, race, place of birth, residence, language, caste or community or any other ground whatsoever, feelings of enmity, hatred or ill will between different religious, racial, language or regional groups or castes or communities"[67] commits an offence under the provision.

Note that both these provisions, i.e.., subsection (1) as well as (2) of Section 353 includes "electronic means" as the mode of commission of the above-mentioned offences. The provision however does not include acts of sharing false information if such person who is sharing it honestly believes that information to be true. The section provides exception to this effect by stating: "—It does not amount to an offence, within the meaning of this section, when the person making, publishing or circulating any such statement, false information, rumour or report, has reasonable grounds for believing that such statement, false information, rumour or report is true and makes, publishes or circulates it in good faith and without any such intent as aforesaid."[68]

These provisions hence can be used to regulate offences such as hoax call warns, online posts with fake contents, etc. Such false contents shared online if can cause terror in the minds of people the offence can be dealt with even by invoking laws related to terrorism. Of recently such hoax bomb threat calls have increased. The government of India has taken up this issue and intends to regulate them with more stringent legal approach. Recently the Civil Aviation Minister expressed concern about such incidences and said that "making hoax bomb threat calls

65 Supra at 7

66 Section 353(1) of BNS

67 Section 353(2) of BNS.

68 Exception to Section 353, BNS

to airlines will be classified as a cognizable offense" and that such calls "significantly disrupting flight operations across the country."[69]

SHARING OF OTHER HATEFUL CONTENT ON VIRTUAL PLATFORM:

According to Section 299 of BNS which has revised Section 295A of IPC, if a person with "deliberate and malicious of outraging the religious feelings of any class of citizens of India, by words, either spoken or written, or by signs or by visible representations or through electronic means or otherwise, insults or attempts to insult the religion or the religious beliefs of that class, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both." This provision thus can be used to regulate online hateful content affecting religious feelings of any class.

ORGANISED CYBER CRIMES:

Crimes committed by a group or on behalf of a group and repeated commission of crimes by such groups now comes under the definition of Organised crime in BNS. The way organised crime and petty organised crimes are defined in BNS makes it broader in its scope so as to include certain forms of cyber-crimes.

Organised Crimes to include some forms of Cyber-crimes:

BNS regulates organised crimes through Section 111, according to which: "*(1) Any continuing unlawful activity including kidnapping, robbery, vehicle theft, extortion, land grabbing, contract killing, economic offence, cyber-crimes, trafficking of persons, drugs, weapons or illicit goods or services, human trafficking for prostitution or ransom, by any person or a group of persons acting in concert, singly or jointly, either as a member of an organised crime syndicate or on behalf of such syndicate, by use of violence, threat of violence, intimidation, coercion, or by any other unlawful means to obtain direct or indirect material benefit including a financial benefit, shall constitute organised crime.*"

It is important to note that the provision apart from expressly mentioning cyber-crime also covers certain other offences which can be committed both in the offline as well as online domain such as – contract killing which can be committed by using online mode while planning the commission of crime or making communication or payment related to the offence by using

69 Piyush Mishra, Hoax calls to be made cognisable offence, situation sensitive: Aviation Minister, https://www.indiatoday.in/india/story/union-aviation-minister-ram-mohan-naidu-hoax-bomb-threat-calls-cognisable-offence-perpetrators-nofly-list-2620414-2024-10-21, last updated on Oct 21, 2024, visited on 17th February 2025

electronic modes or online platforms including dark web. Hence if a person is involved with a group which commits organised crimes including cyber-crimes he can be booked under this provision, which makes the offence more serious compared to a crime committed by an individual that too for the first time. Organised crime under BNSS is a non-bailable offence and hence can become legally a basis to detain the accused in custody pending criminal process. Also, the code defined "economic offence" that which "includes criminal breach of trust, forgery, counterfeiting of currency-notes, bank-notes and Government stamps, hawala transaction, mass-marketing fraud or running any scheme to defraud several persons or doing any act in any manner with a view to defraud any bank or financial institution or any other institution or organisation for obtaining monetary benefits in any form". Most of the offences recognised as economic offence are also the ones that can be committed with the use of electronic mode such as forgery, fraud, etc.

Petty Organised Crimes: BNS defines Petty organised crimes at that which includes offences in form of online cheating, unauthorised sale of tickets, etc. According to Section 112 of BNS 'Petty organised crime' is defined as follows: "(1) Whoever, being a member of a group or gang, either singly or jointly, commits any act of theft, snatching, cheating, unauthorised selling of tickets, unauthorised betting or gambling, selling of public examination question papers or any other similar criminal act, is said to commit petty organised crime." Since these offences of cheating, unauthorised sale of tickets can be committed on online platform, they can be regulated through this provision too. The provision also includes offences of illegal gambling or unauthorised betting, etc which can also be committed on cyber space.

DOCUMENT RELATED CRIMES:

IPC too had provisions through which offences related to or against documents were covered, such as forgery, using false documents, etc. Yet BNS makes the law in this regard wider now since it has redefined the term document under section 2(8) **"document"** as "means any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, and includes **electronic and digital record**, intended to be used, or which may be used, as evidence of that matter."

Manipulating electronic documents: According to Section 201 of BNS if a public servant who is in charge of framing or preparing or translating a document including an electronic record, incorrectly frames, prepares or translates such document or electronic record commits an offence if such act leads to causing of an injury to any person. In addition to this provision, ffollowing provisions of BNS are also related to document related crimes:

- Section 182 [replacing Section 489E of IPC]: Making or using documents resembling currency-notes or bank notes

- Section 183 [replacing Section 261 of IPC]: Effacing writing from substance bearing Government stamp, or removing from document a stamp used for it, with intent to cause loss to Government.

- Section 335 [replacing Section 464 of IPC] defines 'Making a false document". This definition includes "dishonestly or fraudulently" making or transmitting any electronic record or part of any electronic record[70]; affixing any electronic signature on any electronic record[71] and making any mark denoting execution of a document or the authenticity of the electronic signature[72] "with the intention of causing it to be believed that such document or part of document, electronic record or electronic signature was made, signed, sealed, executed, transmitted or by whose authority he knows that it was not made, signed, sealed, executed or affixed."[73]

- Section 336 [replacing Section 463 of IPC] defines Forgery which also includes forging an electronic record.

- Section 337 [replacing Section 466 of IPC] covers the offence of forgery of record of Court or of Public register.

- Section 338 [replacing Section 467 of IPC] covers the offence of forgery of valuable security, will, etc.

- Section 339 [replacing Section 474 of IPC] criminalises Having possession of document described in section 337 or section 338, knowing it to be forged and intending to use it as genuine.

- Section 340 [replaces Section 470 of IPC] states: "(1) A false document or electronic record made wholly or in part by forgery is designated a forged document or electronic record. (2) Whoever fraudulently or dishonestly uses as genuine any document or electronic record which he knows or has reason to believe to be a forged document or electronic record, shall be punished in the same manner as if he had forged such document or electronic record."

- And others.

70 Section 335(A)(ii) BNS

71 Section 335 (A)(iii) BNS.

72 Section 335 (A)(iv) BNS.

73 Section 335 (A)

DIGITAL ARREST:

Cyber-crime in form of digital arrest is nothing but wrongfully restraining or confining a person. This offence can be dealt with by using provisions related to wrongful restraint or wrongful confinement as the case may be. These offences are covered under provisions from section 126 and 127 of the BNS. Also, in most of the digital arrest cases the accused pretends to be a public servant such as a police officer, or a customs officer or a judge etc. Such act of misrepresentation can be dealt with as per Section 204 of BNS according to which: "Whoever pretends to hold any particular office as a public servant, knowing that he does not hold such office or falsely personates any other person holding such office, and in such assumed character does or attempts to do any act under colour of such office, shall be punished with imprisonment of either description for a term which shall not be less than six months but which may extend to three years and with fine." This provision in fact is a revision of Section 170 of IPC and it is been revised to include enhances punishment of imprisonment which an go up to 3 years in addition to fine.

Following provisions may also be used in the cases of digital arrest, however depending upon the facts and circumstances of the case:

- Section 308 of BNS which replaces Section 383 of IPC through which it punishes the of Extortion [explained later]
- Section 351 of BNS which replaces Section 503 of IPC through which it punishes the offence of online harassment or intimidation. [explained later]

CYBER SLAVERY:

Cyber Slavery involves trafficking of person by practising fraud or deception or at times even force or threat. This hence can be dealt with by using provisions from BNS related to trafficking of person, which is covered under Section 143. A person habitually involved in such offence can be punished under section 145 of BNS. According to section 146 of BNS a person who compels another to labour against his will is punishable.

CRIMES AGAINST ONLINE PROPERTIES

It is interesting to note that BNS widens the definition of the movable property by defining it as that which "includes property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth."[74] Earlier IPC

74 Section 2(21) of BNS.

under Section 22 had defined movable property in a very narrow sense as it stated "The words "movable property" are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth." Since IPC had restricted the meaning of movable property to only corporeal property it could not be extended to include incorporeal property such as intellectual property, data and other digital assets.

Theft: According to Section 303 of BNS, which replaces Section 378 of IPC theft is defined as dishonestly taking any movable property.

Snatching: BNS has for the first time criminalised the offence of Snatching under Section 304, according to which "(1) Theft is snatching if, in order to commit theft, the offender suddenly or quickly or forcibly seizes or secures or grabs or takes away from any person or from his possession any movable property."

Extortion: Section 308 of BNS which replaces Section 383 of IPC criminalises Extortion. The provision defines extortion as intentionally putting any person in fear of any injury to that person, or to any other, and thereby inducing that person to deliver any property including any valuable security or anything signed or sealed. BNS provides a clarification to the effect that it includes online extortion too by way of adding a statutory illustration. Illustration (e) under Section 383 states: "(e) A threatens Z by sending a message through an electronic device that "Your child is in my possession, and will be put to death unless you send me one lakh rupees." A thus induces Z to give him money. A has committed extortion." Also note that depending upon the facts of the case, this provision may also be used in a case of digital arrest.

Hence with the expansion of the definition under BNS, the provisions related to theft, snatching, extortion, etc can now be extended to include certain forms of cyber crimes such as data theft, stealing other digital assets and intellectual property, etc.

ONLINE HARASSMENT OR INTIMIDDATION:

According to Section 351 of BNS which replaces Section 503 of IPC, "(1) Whoever threatens another by any means, with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation." Insertion of words "by any means" in this provision makes this provision wider enough to cover online intimidation. This provision too may be used, if necessary, in a case of digital arrest.

Also sharing any content online with the intention of provoking another to break public peace of to commit any offence can be punished under Section 352 which is a revised version of Section 504 of IPC. Section 352 of BNS now has added the words 'in any manner' thereby covering under its ambit online activities including sharing any online post / using any other social media or online platform to share a post that has contents provocative as per the description provided in the section.

FAILURE TO PROVIDE DATA OR OTHER ELECTRONIC RECORDS: Criminal Procedure Code on one had empowered public servants and courts to procure documents or other materials essential to conduct investigation, inquiry or trial through section 91, 92, 93, etc. Non-adherence to their orders for production was an offence as per IPC including as per section 175. BNS now through Section 210[75] which replaces Section 175 of IPC expressly mentions electronic record as that which can also be procured by such public servants and failure to provide such records amounts to an offence under this provision. This provision is an important provision in today's context since often public servants including police officers in the course of conducting an investigation or other legal proceedings including judicial proceedings may require access to data or other information which is in the possession of an internet intermediary or an industry etc. If such industry or internet intermediary fails to provide such data or electronic record it can be considered as a crime as per section 210 of BNS. This provision is however subject to the provisions of Digital Personal Data Protection Act of 2023 [which is yet to be implemented], Information Technology Act of 2000, Intermediary guidelines, etc.

FAILURE TO FURNISH INFORMATION: According to Section 211 of BNS which replaces Section 176 of IPC: "Whoever, being legally bound to give any notice or to furnish information on any subject to any public servant, as such, intentionally omits to give such notice or to furnish such information in the manner and at the time required by law,– (a) shall be punished with simple imprisonment for a term which may extend to one month, or with fine which may extend to five thousand rupees, or with both; (b) where the notice or information required to be given respects the commission of an offence, or is required for the purpose of preventing the commission of an offence, or in order to the apprehension of an offender, with simple imprisonment for a term which may extend to six months, or with fine which may extend to ten thousand rupees, or with both; (c) where the notice or information required to be given is required by an order passed under section 394 of the Bharatiya Nagarik Suraksha Sanhita, 2023 with imprisonment of either

75 According to Section 210 of BNS: "210. Whoever, being legally bound to produce or deliver up any document or electronic record to any public servant, as such, intentionally omits so to produce or deliver up the same,– (a) shall be punished with simple imprisonment for a term which may extend to one month, or with fine which may extend to five thousand rupees, or with both; (b) and where the document or electronic record is to be produced or delivered up to a Court with simple imprisonment for a term which may extend to six months, or with fine which may extend to ten thousand rupees, or with both."

description for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both."

On the other hand according to Section 239 of BNS which has replaced Section 202 of IPC, if a person "knowing or having reason to believe that an offence has been committed, intentionally omits to give any information respecting that offence which he is legally bound to give, shall be punished with imprisonment of either description for a term which may extend to six months, or with fine which may extend to five thousand rupees, or with both." There are similar provisions in Protection of Children from Sexual Offences Act, 2013 too which obligates a person including an Internet Service Provider to inform police about any cases of child abuse on their platform that are within their knowledge.

FURNISHING FALSE INFORMATION: If a person who is legally bound to furnish any information to a public servant, but furnishes false information deliberately can be punished under Section 212 of BNS which has replaced Section 177 of IPC. This provision too like Section 211 can be extended to scenarios where an Internet Service Provider or a person who is obliged to share necessary data with the state agencies [that is public servant] or anybody else deliberately shares false information such as false or erroneous data or wrong IP address, etc. Further, if such false information is shared while being under oath, punishment can be imposed under section 216 of BNS which has replaced section 181 of IPC. Also, if such false information is shared deliberately in order to cause a public servant to use his lawful power to injury of another person, h can be booked under section 217 of BNS which has replaced Section 182 of IPC. Similarly, there are many other provisions to regulate the offence of giving false evidence under BNS. BNS through section 240 which has replaced Section 203 of IPC punishes the offence of giving false information respecting an offence committed, which includes information related to cyber crimes too. Destroying any evidence including documentary evidence is an offence according to Section 241 which has replaced Section 204 of IPC. This provision through BNS has now been amended to include destruction of electronic record 'with the intention of preventing the same from being produced or used as evidence.'

OFFENCES RELATED TO OBSCENITY: While Information Technology Act of 2000 deals with offense of cyber pornography and obscenity under Section 67 and 67A, IPC had provisions related to sale or other similar acts of distribution or publication of obscene book, pamphlet, paper, etc. BNS in its revised version under Section 294 which replaces Section 292 of IPC now includes offences committed by using a content in 'electronic form' thereby covering under its ambit such crimes committed over cyber space or committed with the use of electronic gadgets.

COUNTERFEITING RELATED OFFENCES: BNS through provisions from Section 178 to Section 188 deals with offences related counterfeiting which are often committed with the use of

cyber technology, thereby bringing under the ambit of these provisions' offences committed on the online platform or by using electronic devices.

CONVENTIONAL CRIMES AMOUNTING TO CYBER CRIMES: IPC in its format itself was used to deal with various forms of cyber-crimes including those crimes where were also in form of conventional crimes, such as forgery, fraud, cheating etc. Respective offence's related provisions could be used even to regulate e-forgery, online frauds, online cheating etc. Similarly, defamation too. However, the provision related defamation now includes cyber defamation more explicitly under section 356 of IPC which has replaced Section 499 of IPC since the provision now uses the words "in any manner" so as to include online publication of defamatory content. Thus, the Indian Criminal Substantive law in its current version of BNS has various provisions through which various forms of cyber-crimes can be regulated.

APPLICABILITY OF MULTIPLE LAWS:

While the Information Technology Act was passed in the year 2000 to legalise e-commerce and e-governance the Act underwent significant changes in 2008 thereby covering the provisions relating to cyber-crimes. Yet in cases of various forms of cyber–Crimes IPC was used. Similarly, today BNS too becomes relevant in terms of regulating cyber-crimes. As long as both IT Act and IPC or its current version BNS are in consistency with each other both laws can be used to charge the offenders. According to Section 1(6) of BNS which has replaced Section 5 of IPC: "Nothing in this Sanhita shall affect the provisions of any Act for punishing mutiny and desertion of officers, soldiers, sailors or airmen in the service of the Government of India or the provisions of any special or local law." Hence the police while registering a FIR or courts while framing charge or while convicting can make use of the relevant provisions of BNS and thereby regulate various forms of cyber-crimes.

CONCLUSION AND SUGGESTION:

Since cyber-crime as a term is too wide and covers under its ambit various offence including some offences that emerged with the cyber technology as well as some conventional crimes which though were known to us even before cyber technology became a tool for its commission, to deal with such offences a single law is not enough. Hence in addition to Information Technology Act of 2000, other laws including BNS becomes an important legal framework in the country through which various forms of cyber-crimes can be regulated.

This write up is an attempt to provide a description of some of such provisions from the newly introduced Bharatiya Nyaya Sanhita.

Cyber Offences: Challenges and How We Combat Them

Shri BVS Saikrishna, Ex IRS, CEO, Saptang Labs, Chennai

INTRODUCTION

The rise of digital technologies has transformed the nature of crime, leading to a surge in cyber offences. These crimes, which include hacking, identity theft, cyber fraud, and cyber terrorism, often transcend national boundaries, making their investigation highly complex. Law enforcement agencies face numerous challenges, including jurisdictional conflicts, difficulties in collecting and preserving cyber evidence, and the need for specialized forensic techniques. Despite these challenges, successful investigations have demonstrated the importance of robust cyber forensic methodologies and international cooperation.

(i) Combating cyber crimes remains a challenge due to several factors:

- Anonymity and Global Reach – Cybercriminals often operate anonymously from different jurisdictions, making enforcement difficult.
- Rapid Evolution of Cyber Threats – Criminal techniques, such as phishing, deepfake technology, and artificial intelligence-driven frauds, continue to evolve.
- Lack of Awareness and Reporting – Many victims fail to report cyber crimes due to a lack of awareness or fear of legal repercussions.

(ii) Jurisdictional concerns in Investigation and Registration of Cyber Crime

One of the most significant hurdles in investigating cyber offences is jurisdictional ambiguity. Unlike traditional crimes, cyber crimes are often transnational, with perpetrators operating from different countries. This raises key challenges:

- Lack of Clarity on Jurisdiction – Many cyber offences involve victims and offenders located in different jurisdictions, making it unclear which country has the legal authority to investigate and prosecute.
- Extraterritorial Cooperation – Mutual Legal Assistance Treaties (MLATs) and international agreements are required to access data stored in foreign jurisdictions, often leading to delays in investigation.

- Dark Web and Anonymity – Cybercriminals frequently use Tor networks, VPNs, and encrypted communication tools, masking their identities and locations, making it difficult to trace their origin.

To address these challenges, India has incorporated Section 75 of the IT Act, 2000, which provides for extraterritorial jurisdiction if the offence impacts Indian citizens or systems. However, global collaboration through Interpol, Europol, and the Budapest Convention on Cybercrime remains crucial for efficient investigation.

(iii) Gathering and Preserving Digital Evidence

Digital evidence plays a crucial role in cyber crime investigations but poses unique challenges:

- Volatility of Digital Evidence – Unlike physical evidence, digital records can be easily altered, deleted, or overwritten, requiring timely collection and preservation.
- Encryption and Data Protection Laws – Many cyber criminals use strong encryption, and companies storing data are often bound by privacy laws, making access difficult.
- Chain of Custody – Maintaining a proper chain of custody is essential to ensure that cyber evidence remains admissible in court. Any break in the documentation process can lead to the evidence being challenged.

(iv) Cyber Forensics: Investigating and Securing Digital Evidence

Cyber forensics is a critical component in cyber crime investigations. It involves retrieving, preserving, and analyzing electronic records without compromising their integrity. Key aspects of cyber forensics include:

- Digital Device Seizure – Law enforcement agencies must follow specific protocols while seizing electronic devices to prevent tampering or accidental loss of data. The Information Technology Act, 2000, and the Bharatiya Sakshi Adhiniyam, 2023 (BSA) outline procedures for handling digital evidence.
- Metadata and Log Analysis – Examining system logs, timestamps, and user activities to reconstruct events leading up to the cyber offence.
- AI and Big Data in Cyber Forensics – Modern investigations leverage AI-powered tools to analyze vast amounts of data and detect anomalies in cyber activities.
- Cloud Forensics Challenges – Many cyber crimes involve data stored on cloud servers, requiring cooperation from cloud service providers to access logs and metadata.

(v) Unveiling Digital Offenders

Despite the challenges, we have investigated and have managed to identify cyberfrauds on a day to day basis. A lot of our investigation has uncovered multiple well-organized and systematically coordinated networks that leverage multiple channels and advanced techniques to sustain its operations while evading detection. These networks strategically utilizes social media platforms, multiple email accounts, and deliberate renaming practices to maintain adaptability and ensure continuity.

We utilize advanced algorithms capable of detecting patterns and keywords linked to fraudulent activities. We have also successfully identified multiple bank account numbers and UPI Ids. We have successfully identified 1.5Lakhs of UPI IDs engaging in fraudulent activities. We have also identified phone numbers that are linked to such networks committing cybercrime. We provide detailed reports and real-time data that aid various agencies. We have not only identified and also successfully taken down social media accounts and fake domains created by frauds.

Our forensic and intelligence platform designed for law enforcement, enterprises, and startups integrates data fusion, interaction mapping, and intelligence gathering to enhance investigative capabilities along with enabling real-time data processing and forensic analysis. We bolster In-house analytics and visualization platforms for quick, efficient results. Financial Crime Investigations and Asset Tracing & Recovery has become our forte with the help of our platform.

A lot of regulatory measures have been taken over the years yet cyber crimes have only increased and the modus operandi of them is changing. Keeping up-to-date with the latest trends in this regard has been the backbone of our process.

CONCLUSION

Cyber crime investigations present unique legal and technical challenges, particularly in jurisdiction, evidence collection, and forensic analysis. While Indian laws, such as the IT Act, 2000, and the Bharatiya Nyaya Sanhita, 2023 (BNS), provide a legal foundation, international cooperation and technological advancements are essential to keep pace with the evolving threat landscape. Through enhanced cyber forensic techniques, cross-border legal coordination, and real-time intelligence sharing, law enforcement agencies can effectively combat cyber offences and ensure digital security in an increasingly interconnected world.

Appreciating Digital Evidence: Nuances, Challenges and Changing Legal Scenario

Rajeev Kumar Singh [76] *& Dr. Pramod Kumar Tiwary*[77]

I. **Introduction:** Today, every action of our daily lives has some cyber element in it. Information and Digital technologies have permeated our lives in such a manner that absolute privacy has become a myth; almost every individual in the society is leaving E Footprints every now and then. We live in a tangible world wrapped in an invisible web of digital networks. Information and Digital Technologies and our daily lives have become so intrinsically related that Digital Evidences have gained great importance. Almost every Office, Educational institutions, Hospitals, Railway Stations, Airports, Courts and other public places have CCTV cameras, Computers and Internet connections and all our day today activities and actions are being recorded and stored either in the local databases, severs or cloud. Modes of transport, communication, social and business activities work largely through digital platforms. Digital devices are being used and handled by every individual and organization. As we know that civil wrongs and criminal activities are outcomes of our daily human activities and if some crime is committed or a civil dispute arises digital evidences play a pivotal role in deciding the matters. Increasing instances of cyber-crimes and offences and wrongs committed either through digital devices or on digital platform need special rules and new approaches towards appreciation of evidence in the modern era. The traditional Law of Evidence and mode of proof were largely dependent upon either oral or documentary evidences, but the present scenario shows a paradigm shift from the traditional approach in admissibility and appreciation of Evidence. The face of basic principles of relevancy, admissibility and appreciation of evidence has changed due to technological innovations, but the rule of best evidence still survives. Now the scope and ambit of work of an adjudicator has widened as a basic technological knowledge is expected from him besides the knowledge of legal domain and rules of evidence. This article is a small effort towards examining the changing nuances of Law of Evidence, identifying the present Legal Challenges and suggesting ways of Appreciation of Digital Evidence.

II. **Appreciation of Evidence (Meaning):** Simply the expression 'Appreciation of Evidence' means analysing and assessing the worth, value and quality of a particular piece of

76 Secretary, DLSA, West Singhbhum at Chaibasa

77 Assistant Professor, Faculty of Law, Delhi University

Evidence. "The Process by which a Judge concludes, whether or not a fact is proved is called appreciation of evidence. It is duty of the Court to appreciate evidence minutely, carefully and to analyse it[78]". The Appreciation of Digital or Electronic Evidence requires strict adherence to legal standards and an understanding of technology to effectively utilize such evidence in Court.

III. Legal Perspective on Admissibility and Appreciation of Digital Evidence: Some of the relevant terms like "electronic form", "electronic records", "information" and "secure electronic record" have not been defined in the Indian Evidence Act, 1872 but they have been defined in the Information Technology Act, 2000. From the perspective of Digital Evidence, terms such as "communication device", "computer", "computer resource", "computer system", "data" etc. defined in the Information Technology Act, 2000 are also of great importance. Before discussing the rules regarding admissibility of Digital Evidence, it is important to discuss the definition of "electronic records".

Electronic Record means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche. Therefore, it can be said that any form of data generated, stored, sent or received in form of image, sound or film etc. through a computer can be treated as electronic record. In the context of Digital Evidence it can be said that the difference between computers and communication devices have diminished. Now the work of computers can be done by the smart communication devices and all functions of communication devices could be performed by a computer. Therefore, the ambit of the word computer has greatly widened and all the data generated, stored, sent or received by communication devices or computers or computer network could be termed as electronic record. Therefore, a cell phone, personal computers, desktops, laptops, tablets, smart watch, CCTVs, servers, workstations, mainframes and supercomputers and all other devices performing the functions of computers are computers and the outcome of their working such as video footage, social media posts, CCTV footages, Emails, sound recorded on CDs, DVDs and CDRs are electronic record, which has to be appreciated by Courts for proving or disproving a disputed fact. The Indian Evidence Act lay down special rules with regard to evidence relating to electronic record[79] and their admissibility[80]. As per the provisions of section 65-B (4) of the Indian Evidence Act, production of a certificate is sine qua non for admissibility of an electronic record. The law with regard to the need of production of certificate under section 65-B has been interpreted time and again by the Hon'ble Supreme Court through its various decisions.

78 Kajal Sen v. State of Assam AIR 2002 SC617

79 Section 65-A of The Indian Evidence Act, 1872

80 Section 65-B of The Indian Evidence Act, 1872

In ***State (N.C.T. of Delhi) v. Navjot Sandhu @ Afsan Guru***[81] the Hon'ble Apex Court while dealing with the call records and printouts of the computerized record held that "Section 65 enables secondary evidence of the contents of a document to be adduced if the original is of such a nature as not to be easily movable. Thereafter, in ***Anvar P.V v. P.K. Basheer & Others***[82], The Hon'ble Apex Court held that if an electronic record as such is used as primary evidence under Section 62 of the Evidence Act, the same is admissible in evidence, without compliance of the conditions in Section 65B of the Evidence Act. While so, in ***Shafhi Mohammad v. The State of Himachal Pradesh***[83], The Honb'le Supreme Court relaxed the condition of production of certificate under section 65-B of the Evidence Act and held that "The applicability of procedural requirement under Section 65B (4) of the Evidence Act of furnishing certificate is to be applied only when such electronic evidence is produced by a person who is in a position to produce such certificate being in control of the said device and not of the opposite party." The Hon'ble Apex Court in ***Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal***[84], held that Section 65B does not speak of the stage at which such certificate must be furnished to the Court. The Bhartiya Sakshya Adhiniyam, 2023 was notified in the Gazette of India on 25th December, 2023 and came into force on 1st July, 2024 which has replaced the Indian Evidence Act, 1872 intends to widen the scope of admissibility of Electronic or Digital Evidence. This legislation, inter alia, provides as under:-

(i) it provides that "evidence" includes any information given electronically, which would permit appearance of witnesses, accused, experts and victims through electronic means;

(ii) it provides for admissibility of an electronic or digital record as evidence having the same legal effect, validity and enforceability as any other document;

(iii) it seeks to expand the scope of secondary evidence to include copies made from original by mechanical processes, copies made from or compared from the original, counterparts of documents as against the parties who did not execute them and oral accounts of the contents of a document given by some person who has himself seen it and giving matching hash value of original record will be admissible as proof of evidence in the form of secondary evidence.

(iv) it seeks to put limits on the facts which are admissible and its certification as such in the courts. The proposed bill introduces more precise and uniform rules of practice

81 2005 (11) SCC 600

82 AIR 2015 Supreme Court 180

83 (2018) 2 SCC 801

84 (2020) 7 SCC 1

of courts in dealing with facts and circumstances of the case by means of evidence[85]. So far as rules regarding admissibility of Electronic records are concerned the same provisions with certain modifications have been saved with certain additions under sections 62 and 63 of the present law. The necessity of Certificate as a prerequisite for admissibility has also been retained.

Section 61 of The Bhartiya Sakshya Adhiniyam is a new provision which states that nothing in this Adhiniyam shall apply to deny the admissibility of an electronic or digital record in the evidence on the ground that it is an electronic or digital record and such record shall, subject to section 63, have same legal effect and validity and enforceability as other document. In addition to the above the newly enacted Bhartiya Nagrik Suraksha Sanhita replacing the Code of Criminal Procedure also stresses on the need of adopting the use of digital means and audio visual equipment for collection of evidence in the criminal investigations.

IV. Use of Cyber Forensics: Identification, Analysis and Interpretation of Digital Evidences: Cyber forensics is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any judicial or administrative hearing.[86]. Use of suitable technological tools and appropriate investigation methods are necessary to identify the best digital evidence which could have proper probative weight and are easily admissible in Courts.

Stages of the Cyber Forensic Process:

1. **Identification:** Is the first stage in the Cyber Forensic Process, it is aimed to know the nature digital evidence and its relevance with regard to matter under scrutiny.

2. **Acquisition:** The second stage in this process is taking logical backup, copying the directories and files of a logical volume, not to capture deleted files, taking physical backups, i.e., disk imaging/ cloning/mirror image, Exhibit Computer. Government hard disk is to be used to store the Image of the exhibit HDD. By using Write Protection device, the original hard disk can be free from contamination, the original should be exhibited.

3. **Authentication:** If the hash value is justified, the duplicate is authentic. Hash value is an alphanumeric number, it's a digital fingerprint. For the acquisition and verification of hash value, the software Md5 is replaced with SHA2 to calculate hash value

85 Statement of Object and Reasons of Act No. 47 of 2023

86 https://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/law/07._information_and_communication_technology_/10._digital_evidence-broad_principle/et/7566_et_10_et.pdf

4. **Analysis/Interpretation:** It is one of the most crucial stage wherein digital evidences are extracted, processed, and interpreted

5. **Documentation:** Report should clearly list: software's used and versions contain hash results, all storage media numbers, model make, supported by photographs.

6. **Testimony:** This is stage wherein expert opinion is lead.

Common Investigation Mistakes

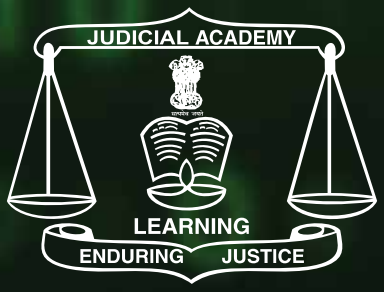
1. Failure to collect and preserve the electronic evidence. The electronic files which are part of captured computer, devices or media must be isolated in a sanitized environment. The replica/mirror image of the hard disks of computers, which have been seized by the investigating authorities, should be deposited with the Court. The Hon'ble Court may take appropriate decision with regard to such replica/mirror image would also be supplied to the accused under s.207 of Cr.P.C./230 of the BNSS,

2. Failure to label the electronic devices/media etc.

3. Failure to calculate the hash function [or value?] of the collected electronic data.

4. Failure to record details of computer forensic examination (s) in the charge- sheet may lead to discharge or even acquittal of the accused.

V. **Conclusion:** The enactment of Bhartiya Nyaya Sanhita (BNS), Bhartiya Nagrik Suraksha Sanhita (BNSS) and Bhartiya Sakshya Adhiniyam is a recent example of law taking note of technological advancements and use and abuse of technology by common man. These three laws will not only help investigators and adjudicators, but the interpretation of newly introduced provisions of these enactments by the Courts in future will not only help to enrich the legal wisdom of the stakeholders but will also help in implementation of laws to achieve the object of administration of justice and crime control. The only need is to focus on capacity building in a techno legal environment for handling the challenges posed by latest technological advancements and increasing use of technology by the society. The proper appreciation of evidence will always remain the most crucial tool for achieving the object of justice in the changing legal scenario.



Prepared by :
Judicial Academy, Jharkhand
Near Dhurwa Dam, Dhurwa, Ranchi – 834004
Phone : 0651-2772001, 2772103, Fax : 0651-2772008
Email id : judicialacademyjharkhand@yahoo.co.in, Website : www.jajharkhand.in