GUARDING THE DIGITAL CYBER REALM OF INDIA: NAVIGATING IPC 1860, BHARATIYA NYAYA SANHITA 2023 AND ITA 2000 IN THE FIGHT AGAINST CYBER CRIME

Bandu B. Meshram[*] And Manish Kumar Singh[**]

[*]Research Scholar, NIMS, School of Law, NIMS University Rajasthan, Jaipur (India).
[**]Head Of Law Department, NIMS, School of Law, NIMS University Rajasthan, Jaipur (India)

Corresponding Author:

Abstract

The research paper explores critical aspects of cybercrime–and the diagnostic & experimentation research for the applicability of IPC 1860/ BNS 2023 in cybercrimes using various cyber court judgements and Information Technology Act 2000 and its amendments. Most of the chapters of "Bharatiya Nyaya Sanhita 2023" are the mirroring chapters of IPC 1860 without straightforward applicability to cybercrimes or hacking or network communication digital crimes. While the IPC provisions are not specifically tailored to cybercrimes, but it can still be relevant in certain situations involving cybercrime. The provisions of BNS 2023 also apply to cyber crimes in India, However how? It is neither explicitly stated in IPC Nor in BNS. The researcher identifies probable IPC 1860 provisions which are also available in BNS 2023 for combating cybercrimes offences. Thus the research critically proves that the Indian Penal Code/ Bharatiya Nyaya Sanhita 2023" shall be adopted in the cybercrime justice systems. The legal interpretation and application of these provisions may vary case to case based on evolving legal standards and precedents.

Keywords: *Cyber Crimes, Abetment, Hacking, Digital Forensic, Punishment*

1. INTRODUCTION

According to Bentham, "offences are prohibited activities by Government legislatures for good or for bad reasons." According to Austin, "a wrong is pursued as civil injury at the discretion of the injured party by his representatives; a wrong is pursued as crime by the sovereign or his subordinates.." According to Paul W. Tappen, "an intentional act in the violation of criminal law, without the sanctioned by the law as felony or misdemeanour is known as crime." The term "Digital Realm" refers to the digital or virtual space, encompassing various computer systems, online platforms, distributed systems, wired and wireless communication, cloud systems, data ware housing, mobile systems, IOT networks, Private and public computing infrastructure and technologies, networking and the like. In hacking experiments[1] , five steps are used-reconnaissance , foot printing, scanning: enumeration, maintaining and covering tracks access are performed using available resources. Hacking Methodology(sec 66 ITA) consists of the steps: Reconnaissance is to know the target computer systems IP Address Range, Network, DNS records, etc. Foot printing refers to the process of gathering information and intelligence about a specific target or system in order to gain a deeper understanding of its infrastructure, configuration, and potential vulnerabilities. Scanning phase includes the usage of tools like, port scanners, network mappers, and vulnerability scanners to scan data for seeking any information like IP addresses, and user accounts to perpetrate attacks on the computer systems. Enumeration refers to the process of identifying and listing all the devices, systems, files, and other digital artefacts present within a given environment or investigation scope. Maintaining Access: After gaining the access of the hacked computer systems, hacker maintain the access of the hacked systems for future exploitation of the computing resources using the owned system known as a zombie system. Covering Tracks: Once the attacker has compromised a system, the attacker would be required to remove the traces of his/her identity in the system to prevent being tracked by authorities by clearing out the system logs, event logs etc. Clearing tracks includes clearing out Sent emails, clearing web server, application server, database server logs, registry contents, by deleting evidence of cybercrime. Thus due to hacking and wired and wireless digital communications, the virtual space is vulnerable to cyber threats, and a wide range of cyber offenses, including but not limited to[2,3]: (i) network attacks (ii) Phishing (iii)Malware attacks(iv) Identity Theft (v) Online Fraud(vi) Cyberbullying and Harassment(vii) Application attacks &Data Breaches(viii) Cyber Espionage(ix) Cyber Terrorism and (x) defamation &the like. The hackers can use artificial intelligence[4] (AI) to create malicious software, phishing emails and spread fake information "Guarding" denotes the crime laws act of safeguarding, protecting, and ensuring the security of the digital space. The Indian Parliament passed the Information Technology Act(ITA) 2000 based on the united Nations Model Law, 1997. Overall, while Sections of the IPC might offer some protection in certain scenarios involving cybercrimes, the primary legal provisions relating to cybercrime investigation, prosecution, and prevention are found in the Information Technology Act, 2000, and other relevant laws. For example: Section 66 ITA prohibits cyber hacking[5] and prescribe punishment and section 65 ITA prohibits tampering source code[5] and prescribe punishment.

According to cybersecurity firm CloudSEK report, India is the biggest target for cyber attacks after the united states in 2021 and 2022 with nearly 500 attacks last year dated July 24, 2023. NordVPN,a virtual private network service provider finds that India was the worst hit by data breatches like data stolen and sold on bot markets of more than 600,000 .

Digital experts warned it also undermines India's aim to develop and export to Asian and African counties its digital public infrastructure Model comprising Aadhar, mobile payment systems UPI and National Health stack data platform.

2. Parallel Provisions of IPC 1860 and BNS 2023 in Cyber Crimes

The provisions of **IPC 1860 and** Bharatiya Sanhita apply to any offence committed by any person targeting a computer resource. However cybercrime offences are not explicitly stated into the IPC or amendment of IPC which will be called as Bharatiya Nyaya Sanhita 2023. The researcher explicitly identifies how the different concepts of cyber crimes are applicable in both the Acts. Parallel chapters of IPC 1860 in "Bharatiya Nyaya Sanhita 2023"(Amendment of IPC 1860) are shown in Table 1

Table 1: Mirroring chapters of IPC 1860 in Bharatiya Nyaya Sanhita 2023

IPC 1860 and Proposal for cyber offences	**Bharatiya Nyaya Sanhita 2023**
(i)chapter 3 punishment IPC 1860 Sec 75- Enhanced punishment for certain offences under Chapter XII or Chapter XVII after previous conviction.	Chapter ii Of Punishments
(ii) Chapter iv General Exceptions Section 84 in cybercrime and mental incapacity s-120	Chapter Iii General Exception S-22. Act of a person of mental illness
(iii) right of private defence(sec 96-106 against cybercrime-300 Murder ,death, 320 grievous hurt.375 committing rape, 359 , 360 –kidnapping	Of the Right of Private Defence(sec 34-44) Chapter V Of Offences Against Woman And Children Of Sexual Offences
(iv)chapter v of Abetment	Chapter iv Of Abetment, Criminal Conspiracy And Attempt
(v) Chapter va Criminal Conspiracy	S-61. Criminal conspiracy
(vi) Chapter vi Of Offences Against The State(cyber-	Chapter Vii Of Offences Against The State

crime offences against the state)	
(vii) Chapter vii Of Offences Relating To The Army, Navy and Air Force	Chapter viii of offences relating to the army, navy and air force.
(Viii) Chapter viii Of Offences Against The Public Tranquillity	Chapter xi Of Offences Against The Public Tranquillity
(ix) Chapter ixa Of Offences relating to Elections .	Chapter ix Of Offences Relating To Elections
(x) Chapter Xv Of Offences relating to Religion	chapter xvi of offences relating to religion
(xi) Chapter xvi Of Offences affecting the Human Body(how the cybercrime can cause death to the victim of cybercrime?)	Chapter vi Of Offences Affecting The Human Body
(xii) Chapter xvii Of Offences Against Property Theft, Extortion, Robbery and Dacoity, Cheating etc.	Chapter xvii of offences against property
(xiii) Chapter xvii Of Offences Against Property (criminal breach of trust	Sec-314 of criminal breach of trust. chapter xii of offences by or relating to public servants.
(xiv)cheating , personation and trespass	Sec-316.cheating.Sec- 317cheating by personation, Sec-327-of criminal trespass
(xv) Chapter Xix Of The Criminal Breach of Contracts Of Service (cybercrime on the criminal breach of contract of service)	Sec 355. Breach of contract to attend on and supply wants of helpless person.
(xvi) Chapter xxii Or Criminal Intimidation, Insult and Annoyance(cybercrime criminal intimation, insult and annoyance)	chapter xix of criminal intimidation, insult, annoyance, defamation, etc.
(xvii) Section 511 attempt to commit offences in the context of cybercrime.	Attempt to commit ALL offences in Bharatiya Nyaya Sanhita 2023
The researcher provides the mirroring of various sections of The IPC[5,7] with BNS[6] which shall be reliably used to handle the cybercrimes.	

3. Section 53 and Chapter 3 of Punishment

Sec 53: Punishment Chapter 3 of the IPC classifies offenses into various categories, such as offenses against the state, offenses relating to the human body, offenses against property, and so on. Section 53 of the IPC outlines the different types of punishments that can be imposed for various offenses, including cybercrimes using Hacking[8, 8.1]
Cybercrimes involving data theft or financial fraud or cyber terror against state may attract more severe punishments, while cyber harassment or online defamation may have milder penalties. Section 53 IPC addresses various cyber crimes such as (i)Mens Rea and Actus Reus: Like any other criminal offense, cybercrimes require the presence of both mens rea (criminal intent) and actus reus (the criminal act) in internet crimes[9] (ii)Joint Liability: Section 53 of the IPC addresses cybercrimes joint liability with sec 117 IPC for offenses committed by multiple persons. (iii)Attempted Crimes: This concept is applicable to cybercrime cases where an attempted hack, phishing attempt, or data breach can be prosecuted.(iv)Accessories: offenses are relevant in cybercrime cases, where individuals may assist or aid others in carrying out criminal activities online.

Chapter 3(of Punishments) of the IPC also provides for certain exceptions and defenses, which could be relevant in some cybercrime cases such as self-defence, mistake of fact, or acts done under duress. Sec 53 IPC . Punishments. The punishments are death; imprisonment for life; imprisonment- rigorous, or simple ; Forfeiture of property; Fine[10]Punishments for different nature of cyber crimes are also listed in Sec 109 to 120 IPC, accordingly punishment shall be decided.

Section 44 IPC, 1860 provides a broad definition[12] of "injury" . While this provision is not specifically tailored for cybercrime, it is applicable to cybercrimes due to the nature of harm caused in the digital realm. Researcher identifies how this section is applicable in the context of cybercrime:
(i)Bodily Injury: In cybercrime cyberbullying or online harassment that leads to severe emotional distress or self-harm can be considered a form of bodily injury under this provision.(ii)Mental Injury**:** Cyberbullying, cyberstalking, or online defamation can lead to emotional trauma, anxiety, depression, and other psychological distress. (iii)Reputation Injury: Cybercrimes such as online defamation [9]or spreading false information about an individual or business can harm their reputation and social standing.
(iv)Property Injury: Cybercrimes can also cause damage to property, that result in data breaches, destruction of digital assets, or unauthorized access[12] to computer systems affecting the confidentiality, integrity and availability of Data[13, 14]
When dealing with cybercrime cases, law enforcement and the judiciary consider both the provisions of the IPC (including Section 44) and the relevant provisions of the IT Act 2008- Section 66A- cyberbullying and sending offensive messages online.

Section 66B- cyberstalking or harassment and Section 66D: impersonation using a computer resource-in cybercrime can have serious impact related to financial loss, damage to reputation, and the like. Accordingly appropriate charges are framed, and appropriate penalties are imposed based on the nature of the offenses and the harm caused to the victim.

4. Section 84 in Cybercrime and Mental Incapacity

To apply Section 84 in a cybercrime case, the following elements need to be established at the time of committing the cybercrime :(i)Unsoundness of mind. (ii)Incapable to know the act due to the mental disorder. **For Example**: In a cybercrime case where the accused is suffering from severe schizophrenia and, during a psychotic episode, hacks into someone's online accounts to access personal information, they might not understand the nature of their actions or realize that it is illegal or morally wrong due to their mental condition. But this can be done through medical records, expert opinions, and psychiatric evaluations.

The Rule In M'Naughten's Case for Mental Incapacity: Defendant, M'Naghten mistook Edward Drummond secretary to the Prime Minister for Prime Minister Sir Robert Peel and shot Drummond by mistake. Section 84 IPC embodies McNaughton rules as follows: if the offence is done by a person having unsoundness of mind, without the knowledge of the act or that he is doing what is either wrong or contrary to the law." House of Lords given the judgement that M Naghten was found not guilty. *In Amrit Bhushan v. Union of India 1976*, the Supreme Court found that the M'Naghten rules define the word "insanity" of the accused whereas under Section 84, IPC describe the word "unsound. India adopted the principles of M'Naghten Rules which became the base of Section 84 IPC.

5. Right Of Private Defence(Sec 96-106 IPC) Against Cyber Crime

In the word of Bentham "The right of private defence is necessary for the protection of life and liberty and property." Section 96 to 106 IPC states the law relating to the right of private defence of person and property.

Section 97 can be useful in protecting computing property and assets such as (i)Protection against unauthorized access (Sec 43(a) ITA)-criminal as well as civil liability of the criminal)of your computing property, such as your computer system, website, or online accounts,(ii) Prevention of data theft(Sec 43(b) ITA+Sec 378IPC define Data theft) stored on your computing devices or servers.(iii) Defense against hacking attempts or malware infection.(iv) section 383 IPC define extortion (which is not defined in ITA) for protection from cyber extortion to obtain payment. Cyber extortion types are Sextortion ,Email extortion ,Blackmail, Spear phishing , Denial of Service (DOS), ransomware Attack (v)Securing online banking or financial accounts transactions.

(vi)Defending against denial-of-service (DoS)[4] attacks to disrupt your online services or computing assets., you can exercise your right of private defence to prevent or minimize the impact of these six attacks. It is essential to note that while Section 97 grants the right of private defence, there are certain limitations to this right as outlined in Sections 99 and 105. Sec 43(f) ITA 2000 read with Sec 66 ITA provides punishment for DoS attacks where compensation for the victim is upto 5 Crore with adujucationg officer and above five crore with civil court . while imprisonment. to the abuser is upto 3 years and fine upto 5 lakh and with both.

Section 98 IPC :Right of private defence against the act of a person of unsound mind etc[12]. If a person with an unsound mind commits a cybercrime unintentionally or unknowingly, the accused may assert their right of private defence[12] against such an act under following situations:(i)Protection against unintended actions due to mental illness, intoxication, or influence of drugs. (ii)Limited applicability: If the act committed by the person, despite being unsound of mind, is considered an offence, then the right of private defence may not apply.(iii)Reasonable use of force: If an individual encounters an individual with unsound mind attempting to engage in cybercrime. In cybercrime incidents involving individuals with unsound minds, it becomes even more essential to involve the appropriate legal authorities and seek expert advice to ensure that the accused's rights are protected while addressing the illegal activity effectively.

Section 99 IPC -no right of private defence. The principles can be relevant to insider cybercriminals such as **(i)** If the insider cybercriminal is a public servant acting in good faith, individuals may not have the right to use private defence against their actions. (ii) If the insider authority or a public servant, is acting as cybercriminal or carrying out cybercrimes, insider individuals may not have the right to private defence against their actions.(iii) If individuals become aware of an insider cybercriminal's activities, but there is sufficient time to report the matter to law enforcement or other public authorities, the right of private defence may not apply. (iv) Even if there is a right to private defence against an insider cybercriminal, the use of force should not be excessive or disproportionate to the threat posed. While Section 99(2) of the IPC can be relevant in digital realm for certain cybercrime scenarios such as (i), theft can include unauthorized access to someone's online accounts or sensitive information with the intention of misappropriating it.(ii)Robbery may involve stealing valuable digital assets, cryptocurrencies, or other valuable data or information through force, intimidation, or deception.(iii)Mischief involve tampering with or altering computer data, disrupting digital systems, or spreading malware to cause damage.(iv)Criminal Trespass can occur when an unauthorized person gains access to a computer or communication network.(v)Attempt to commit cyber crime offences but unsuccessful Offences like unsuccessful hacking.

Thus if the act involves any of the mentioned cyber offences such as theft, robbery, mischief, criminal trespass, or an attempt to commit them, the right of private defence may not be applicable.

Section 100 IPC :The right of private defence of the body extends to causing death: While Section 100 primarily addresses physical encounters, it may have limited applicability such as the principle of proportionality in cybercrime scenarios under certain circumstances like (i)Imminent physical harm: In rare cases, cybercrimes may lead to real-world physical harm or violence. For instance, cyberbullying, online harassment, or cyberstalking might escalate to physical threats or attacks causing death. (ii)Self-defence in the physical realm: Cybercrimes might lead to real-world confrontations where an individual perceives a significant risk of death or grievous bodily harm. If someone is attempting to physically harm the victim as a direct consequence of a cybercrime, the victim may resort to self-defence as provided under Section 100

Section 101: **When such right extends to causing any harm other than death**. In cybercrime cases, the concept of self-defence under Section 101 of the IPC may come into play if an individual is being attacked, threatened, or harmed through digital means. For example, if someone is being subjected to cyberbullying, cyberstalking, online harassment, or other forms of digital threats, they may have the right to defend themselves from such harm subject to the restrictions mentioned in Section 99IPC And If the offence are not Enumerated in section 100 IPC.

Section 102 : Commencement and continuance of the right of private defence of the body : In the context of cybercrime, let's understand how Section 102 may apply:(i)Commencement of Right of Private Defence: If someone reasonably apprehends that they are in danger due to a cybercrime attempt or threat, such as threatening messages or cyberstalking attempts, they can act in self-defense to protect themselves as long as the danger is perceived. (ii)Continuance of Right of Private Defense: if the threat from a cybercriminal is ongoing, the individual may continue to defend themselves until the threat ceases.

Section 103 : When the right of private defence of property extends to causing death :The right of private defence of property extends to causing death under the restrictions mention in section 99 IPC in the following cases (i) robbery or theft, (ii) house-breaking by night(iii) mischief by fire in building, tent and the like (iv) mischief, house-trespass.

In the context of cybercrime, right of private defence of property could apply when someone is trying to hack into or damage their computer systems, networks, or data , software's, systems programs or any other digital assets.

Section 104 IPC – While Section 104 IPC is not directly applicable to most cybercrime cases due to its focus on physical assault, the principles of self-defence outlined in Section 99 of the IPC can still be considered when assessing a victim's actions in response to specific cyber threats that may indicate a credible risk of physical harm, depression or suicide death. Due to (i)cyber assault with physical threat: In some cybercrime cases, the perpetrator might use digital means to threaten physical harm to the victim. For example, if someone sends threatening messages via electronic communication, indicating an intention to physically harm the victim, the victim might claim the right of private defense under Section 104. (ii) cyber extortion: cybercriminals may engage in extortion by threatening to cause physical harm to the victim or their loved ones unless a ransom is paid. Some victims of cybercrimes may suffer with (iii) mental health issues, life stressors, (iv) mental health impact :persistent and malicious attacks on social media, email, or other digital platforms can lead to or a decline in mental well-being (v) lack of support**:** due to fear, shame, or a lack of awareness about available resources and other personal and social circumstances causing death or suicide.

While Section 105 (IPC) primarily relates to **(i)** theft (ii) robbery (iii) criminal mischief or trespass danger to the physical property, its principles can be analogously applied to certain cybercrime cases in India, where digital property or assets are involved. The right of private defense commences to prevent cyber crime actions to counteract the attack and protect their danger to their digital property such as (i) unauthorized access(Sec70ITA) to computer systems, sensitive information, trade secrets, or intellectual property or data breaches, (ii) data theft(Sec 43(b) ITA 2000)or deletion: a cybercriminal attempts to steal valuable data or maliciously delete digital records,. (iii)Cyber Attacks on Protected Systems[section 70, ITA 2000]: When a cyber-attack, such as a Distributed Denial of Service (DDoS) attack, is launched against an individual or organization's computer systems,. This can include deploying defensive mechanisms to mitigate the impact of the attack and prevent further damage. Section 43(f) ITA 2000 provides penalty for the culprits who deny the access to the real user.

Section 106 : Right of private defence against deadly assault when there is risk of harm to an innocent person. When XYZ is attacked by a mob or thief's to murder, grievous hurt ,rape her/him or kidnapping or abducting, XYZ can do his/her private defence by firing on the attacker with risk of harming the attacker , it's essential to understand that in today's digital age, some crimes might have a cyber component or might be facilitated through the use of technology. For instance, cyberbullying, cyberstalking, dissemination of harmful content, or hacking personal information to commit the offenses mentioned in IPC can be considered cyber crimes in table 2.

Table 2 Parallelism between IPC Physical crime with cyber crime

IPC crime (Sections)	Cyber crime to cause IPC Crime
300 Murder:death.	cybercrimes like hacking(Sec 66 ITA) critical infrastructure, launching cyber-attacks on medical facilities, or manipulating systems that control transportation can potentially cause harm, including loss of life. See section 103IPC and 104 IPC for cybercrimes causing death.
320 grievous hurt.	Cyberbullying-harassment of teenagers or children's using technological devices using text messages, voice mail, email and social networking sites. Forms of cyber bulling are Insulting, targeting, identity theft, excluding either online or offline, harassment, loading or sharing images, videos[15](Sec 66A of ITA Read with Sec, 500,506 7507 IPC), cyberstalking, or any online activity that incites violence or leads to physical altercations can potentially cause grievous hurt.
375 committing rape.	in the context of cybercrimes, there are offenses that may be related to sexual harassment[15](Sec 67-obscence material and 67A ITA Punishment,) exploitation, or non-consensual sharing of intimate content such as Cyber Sexual Harassment, Cyber Voyeurism(revenge porn), Online Grooming with the intention of sexually exploitation, Cyber Extortion, blackmail Online Sexual Exploitation of Children[15,16] or child pornography(Sec 67B ITA 2008 read with Sec 292, 293,294, 500, 506 and 509 IPC).
	IPC Section 359 pertains to the offense of kidnapping: Using electronic means to demand ransom or extort someone with the threat of physical harm or kidnapping. A section 360 deal with the offense of kidnapping includes cyberstalking, cyber harassment, online child grooming, and cyber extortion.

Sec 67 Punishment for publishing or transmitting obscene material in electronic form (Amended vide ITAA 2008) 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.

67 A ITA 2008 Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form (Inserted vide ITAA 2008) Whoever publishes or transmits in the electronic form sexually explicit material shall be punished on first conviction with imprisonment upto to five years and with fine upto to ten lakh rupees and in the event of second or subsequent conviction with imprisonment upto to seven years with fine maximum to ten lakh rupees.

Sec 67 B ITA 2008 Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form shall be punished on first conviction with imprisonment which may extend to five years and with a fine maximum to to ten lakh rupees and in the event of second or subsequent conviction with imprisonment upto to seven years and also with fine upto to ten lakh rupees: Provided that the 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 if it is in the interest of science, literature, art or learning or other objects of general concern; or or used for bonafide heritage or religious purposes.

6.Chapter v Of Abetment IPC

Section 107 IPC deals with abetment of a thing When someone abets a cybercrime, they are not directly involved in carrying out the illegal activity themselves, but they actively participate in promoting or act of aiding, encouraging, or instigating another person to commit a cybercrime or supporting it by providing technical expertise, sharing knowledge about hacking tools or techniques, offering financial support. Hacking steps namely Reconnaissance , Scanning and Enumeration are the cyber crime abetment steps. Abetment and Attempt offence require the text of proximity, where preparation to commit cyber offence (hacking) is considered as offence in 411 of IPC and the Malaysian Computer Crime Act 1997, sec7(2).

For example, if a person provides instructions to someone on how to conduct a hacking attack, they could be held liable under Section 107 of the IPC for abetment of a cybercrime. If someone is found to have abetted a cybercrime, they may face legal consequences, including imprisonment and/or fines, depending on the severity of the offense (Hacking)under Sec 66(1) read with Sec 43 ITA.

7. Criminal Conspiracy- Section 120 IPC

Criminal conspiracy under Section 120- Criminal conspiracy can be invoked when two or more individuals or entities plan and agree to commit a cybercrime together. For example, if a group of individuals plans to launch a coordinated Distributed Denial of Service (DDoS)[14] attack on a specific website, they can be charged with criminal conspiracy under the Indian Penal Code. Cybercrimes encompass a wide range of offenses, such as hacking, data theft, online fraud, identity theft, cyberbullying, online harassment, email frauds. and more.

DOS(Sec 43(f) read with Sec 66 of ITA-compensation to the victim upto 5 Cr. with adjudicating officer and above 5 Cr with civil court. Imprisonment to the attacker is upto 3 years and fine upto 5 Lakhs and with both.IPC sections relevant to criminal conspiracy include:(i)Section 378 IPC : Theft - covers the general offense of theft, cyber theft deals with unauthorised access, hacking, tempering source code ,theft of data or information.(ii)Section 379IPC: Punishment for theft - provides penalties for theft offenses.(ii)Online Fraud: Online fraud can be covered under various provisions, such as:(i)Section 419 IPC: Punishment for cheating by personation.(ii)Section 420IPC: Cheating and dishonestly inducing delivery of property (iii)Section 463: Forgery - when documents are forged in online fraud is known as cyber forgery and frauds cases. Section 65 ITA with Section 464, 465 and 469 IPC deals with document forgery using the digital means like colour printers, scanners and the like.

29A IPC define “Electronic record similar to section 2(1)(f) ITA Sec 464 define false electronic record. 120B IPC. Punishment of criminal conspiracy: offence shall be punishable with death, imprisonment for life or rigorous imprisonment for a term of two years or upwards, or as abetted offence depending on the severity/ nature of offence. In Email frauds(sec 66 read with sec 43(i)), the acts are done dishonestly and fraudulently. Forms of email frauds are phishing(Sec 66-D ITA 2008 and Sec 379 and 420 IPC), Email bombing(Sec43(e), read with Sec 66 ITA & Sec 287 IPC), Email Spoofing(Sec 66D and 417,419, 465 IPC).

State Of Tamil Nadu V. Suhas Katti (2004) : in the case, accused was sending a woman obscene, defamatory and annoying messages in a yahoo message group, the accused individuals were charged with criminal conspiracy under section 120-a and various provisions of the ITA 2000, for hacking into computer systems and committing cybercrimes. In this case a accused writes his name below the email message intending the recipient to consider it as a message sent by that person(accused). This is considered as "Forgery" of an electronic document under section 463 IPC. The

Supreme Court clarified that cybercrimes could be prosecuted under both the IPC and the ITA, and criminal conspiracy could be invoked when two or more individuals conspire to commit a cybercrime. The magistrate in egmore, chennai found the accused guilty of offences under section 469, 509 IPC and 67 of IT Act 2000, accused was sentenced to rigorous imprisonment for 2 years under 469 IPC and to pay a fine of rs.500/-, one year simple imprisonment and Rs 500 fine under 509 IPC and two years imprisonment with a fine of Rs 4,000 under section 67 of IT Act 2000. All sentences were to run concurrently.

8. Cyber Crime Offences Against The State

Cybercrimes can potentially be related to "Offences against the State" under the Indian Penal Code (IPC) when individuals or groups use electronic communication networks or devices to commit acts that threaten the security, sovereignty, integrity, or public order of the state. " Offences against the State" of "Bharatiya Nyaya Sanhita 2023 is the mirroring chapter of IPC.

Some relevant sections of the IPC that may be invoked in such cases include:
Section 121IPC: Waging, or attempting war against the Government of India. This can include cyber-attacks intended to disrupt critical government infrastructure or communication systems or cyber terrorism. The USA passed The Nation Infrastructure Protection Act 1990 to control the cyber terrorism.
(i)State(NCT) OF Delhi Vs. Mohd. Afzal and others 107(2002)DLT 385[16] (Parliament attack case)
(ii) Md. Ajmal Md. Amir Kasab Abu Vs. State Of Maharashtra[17]: 26/11 Mumbai terror attack. Ajmal Kasab was awarded the death penalty, by the Bombay High Court and SC .

Section 121A: This section deals with the criminal conspiracy punishable by Section 121 to wage war against the state, which can be applicable in cases where individuals or groups plan and coordinate cyber-attacks with the intent of causing harm to the state like ransomware attack on AIIMS Delhi or spreading virus or worms into computing systems of government(Sec 43(e) and 43€ read with sec 66, 77 B and 268 IPC.)The USA passed the spyware Control and Privacy Protection Act 2000.

Section 122: Collecting arms, etc., with the intention of waging war against the Government of India. In the context of cybercrimes, this section could apply to the collection or distribution of tools or software used for cyber-attacks against the state. Section 124A: Sedition. This section deals with acts that attempt to bring hatred or contempt towards the Government of India. Online activities such as promoting violence against the state or advocating for its overthrow can fall under this provision.

Section 153B: Deals with giving provocation with intent to cause riot, Imputations, assertions prejudicial to national-integration. This section is applicable when individuals or groups make assertions that promote enmity between different groups to spread riot, leading to a threat, to national integration. In the context of cybercrimes, this can include spreading hate speech or religious matters or misinformation through digital platforms.

Section 505:. This section deals with making statements for public mischief that cause fear or alarm to the public, or promoting enmity, hatred, or ill-will between different religious, racial, language, or regional groups or offences committed in place of worship by dissemination of fake news or malicious content.

Case: State (NCT of Delhi) v. Navjot Sandhu (2005): Commonly known as the "Delhi High Court Blast Case" or "Terrorist Attack on Indian Parliament Case[18]," this case involved a terrorist attack on the Indian Parliament in 2001. The accused were identified with the mobile communication digital evidence to do this crime. The accused were charged under various sections, including Section 121 Section 121A and Section 122 . The offences relates to offences under the IPC are offences against state, relating to defence services, public tranquillity, religion , property and criminal intimation and some special hijacking acts. Under - TADA act, disruptive means any action taken, weather by act or by speech or through any other media or any other manner. The word terrorism is defined in IPC. There is a is a need to incorporate permanent sections to deal with terrorism in all three major acts dealing with crimes, IPC 1860, CrPC1973 and the Evidence Act 1872. The terrorist and disruptive Activities (prevention) Act 1987 (TADA)is repealed in 1995 and the prevention of terrorist act 2002(POTA) is repealed in 2004.. The Unlawful Activities(Prevention) Act 1967(UAPA) amended in 2008.

In Bharatiya Nyaya Samhita 2023 , the new sections are added sec 111-offences of terrorist Act, sec 150 act endangering sovereignty, Integrity and unity of India whereby the cybercrimes can be controlled. 44(b) Penalty for failure to furnish information, shall be not exceeding five thousand rupees for every day . Section 69A ITA authorizes the Central Government to block public access by issuing instructions to any intermediary/ISP in the interest of sovereignty and integrity of India, defense of India, security of the State, and intermediary /ISP who fail to do so shall be punished with an imprisonment upto seven years and fine. 69b ITA authorizes the central government to monitor and collect traffic data for cyber security monitoring and controlling and any intermediary/ISP who knowingly contravenes shall be punished with an imprisonment upto to three years and fine.

9.Offenses Related To The Army, Navy, And Air Force

Offenses Related To The Army, Navy, And Air Force under the Indian Penal Code (IPC) may be relevant to cybercrimes in situations where cyber activities have a connection with the defense forces. For Example (i) Unauthorized Access[19] to Defense Systems(Sec 70 ITA) If someone gains unauthorized access to computer systems, networks, servers or databases belonging to the army, navy, or air force, it could potentially fall under provisions related to unauthorized access to defense systems. This could include accessing sensitive military information, classified data, or compromising the security of defense networks.(ii)Espionage or Disclosure of Sensitive confidential Information[19]: Cyber activities aimed at obtaining or disclosing sensitive military information, trade secrets, or classified data could be considered offenses related to espionage. Such activities might involve cyber espionage or hacking into defense systems to extract confidential information. According to Sec 72 ITA 2000 any person who breach of confidentiality and privacy by disclosing electronic record, information or other material shall be punished with imprisonment upto two years, or with fine maximum to one lakh rupees, or with both.

(iii)Sabotage or Disruption[20]: In this scenario, cybercriminals engage in activities with the intent to sabotage or disrupt the functioning of defense systems, or causing damage to vital infrastructure. For example, disrupting communication networks or critical systems of the armed forces could be covered under these provisions.(iv)Impersonation or Fraud[20]: Cybercriminals who impersonate military personnel, officers, or officials with the intent to deceive and commit fraud could be charged under provisions related to impersonation and fraud.

This might include instances where hackers pose as military personnel to gain access to restricted areas or resources. According to Sec 66D ITA 2008 the person who cheats by personation using electronic communication , shall be punished with imprisonment upto three years and fine up to one lakh rupees. (v)Data Theft[21](Section 378 IPC Defines Data theft) or Misuse or Identity theft (Sec 66 C of ITA Sec 449 IPC): downloading data , sensitive data, trade secrets, or military plans are stolen or misused through cyber means, it could be covered under provisions related to theft, misappropriation, or misuse of confidential information. Sec 43(b)Data Theft ITA[21] makes the person to pay damages upto Rs. One Crore to the victim so affected. Identity theft(vi)Cyber Terrorism[21]: In cases where cyber activities are intended to create fear, panic, or disrupt the functioning of the armed forces or military operations, it could potentially fall under provisions related to cyber terrorism. According to 66F (2) ITA 2008 [21] The punishment for cyber terrorism shall extend to imprisonment for life'.

Indian Air Force Group Captain Arrested for Espionage[22] (2018): In 2018, a Group Captain Arun Marwaha, An Indian Air Force officer was arrested for allegedly sharing sensitive information and documents using social media platforms to Pakistan's Inter-Services Intelligence agents who communicated with him masquerading as women, which could have potentially compromised national security. This case brought attention to the risks associated with insider threats and the use of online platforms for espionage activities.

DRDO's Pune case :The vigilance team at DRDO's Pune facility harboured suspicions that their eminent scientist Pradeep Kurulkar serving as the head of the Research & Development Establishment (Engineers)was engaged in contact with Pakistani Intelligence. Their investigation revealed that he had been exchanging audio and video messages with a female Pakistani Intelligence Operative via WhatsApp. The ATS further alleges that the scientist had reportedly divulged sensitive security and defense-related information to her.

10. Offences Against The Public Tranquillity

Offenses against public tranquillity generally involve acts that disturb the public peace or create a sense of fear, anxiety, or unrest among the general population. Cybercrimes can achieve similar effects in the digital realm, leading to disturbances in public tranquillity. The researcher identifies various actions/ offenses can disrupt the public peace, order, and harmony through digital means and contribute to an atmosphere of fear and unrest among individuals who feel targeted are as below:

(i)Spread of False Information and Panic[24] Certain cybercrimes involve the dissemination of false information, fake news, or rumors through online platforms, social media, or messaging apps. These false claims can lead to panic, confusion, and unrest among the public. For instance, spreading fake news about a potential security threat or disaster could trigger public fear and anxiety, disturbing the public tranquillity.(ii)Cyberbullying and Online Harassment or use of social media[25] (503 IPC (criminal intimidation), 504IPC (to provoke breach of the peace), and 509 IPC (to insult the modesty of a woman): can create a hostile online environment, leading to emotional distress and mental harm for the victims.(iii)Incitement to Violence or Unlawful Activities: Cybercriminals can use digital platforms to incite violence, riots, or other unlawful activities. For instance, organizing or promoting violent protests or riots through online channels can disturb public tranquillity by creating an environment of unrest and instability.(iv)Disruption of Essential Services: Some cybercrimes involve attacks on critical infrastructure, such as power grids, transportation systems, or communication networks. leading to public inconvenience, panic, and unrest as people grapple with the consequences of service outages.(iv)Online Hate Speech Act on social media (Sec 66 ITA, 153(A), 295 IPC File FIR) and Communal Tension: Cybercrimes [21]related to hate speech, causing annoyance, obstruction, intimidation, spreading communal hatred, or promoting enmity between different groups can disrupt the harmony within society and create tensions that disturb public tranquillity.(iv)Fraud and Financial Scams: Certain cybercrimes involve large-scale financial frauds,

Ponzi schemes, or online scams/selling(sec 66 D ITA) that can lead to significant financial losses for individuals. These losses can cause distress and unrest among victims and contribute to a sense of insecurity in the public.

66 A ITAA 2008 offender for sending offensive messages causing annoyance, criminal intimidation, enmity, hatred, through communication service or electronic mail, etc. shall have imprisonment upto two three years and with fine. In Bharatiya Nyaya Samhita 2023 , the separate section is added about Mob Lynching , punishable with 7 years or life imprisonment or death penalty , but cybercrime is not considered.

WhatsApp Mob Lynching Cases **(2018-2019):**In 2018 and 2019, a series of mob lynching incidents were reported in various parts of India. These incidents were fuelled by rumours and misinformation spread through messaging platforms like WhatsApp. False messages about child abductions, organ harvesting, rape, and other sensitive issues were widely circulated, leading to public panic and mob violence. These incidents highlighted the serious consequences of spreading false information through digital platforms and its potential to disrupt public tranquillity. The WhatsApp mob lynching cases false child-kidnapping rumors on WhatsApp serve as a significant example of how cyber activities can contribute to disturbances in public peace and order.

Freedom of speech case ; In *Shreya Singhal v Union Of India*, case while quashing Section 66A ITA 2008, The Supreme Court has not only gave afresh lease of life to free speech in India but has also performed his role as a constitutional court of India and stated that sec 66B and 67C of ITA 2008 are good enough to deal with such cybercrimes.

Section 146 of the IPC : It's possible that in certain situations, cybercrime could play a role in escalating tensions that lead to unlawful assemblies or riots, force and violence . For example, if a cybercriminal orchestrates a large-scale hacking attack that disrupts essential services in a community, such as power or communication systems, the resulting chaos and frustration could potentially contribute to social unrest, leading to protests, demonstrations, or even riots.

Section 147 primarily addresses the punishment for individuals involved in physical acts of rioting and does not specifically address cybercrimes. There could be indirect connections between cybercrime and the potential for escalating tensions or contributing to social unrest. For instance, if a cybercriminal perpetrates actions that significantly disrupt societal norms or essential services, it might lead to civil unrest and demonstrations, which could eventually escalate to the point of rioting.

Section 153A IPC can be related to various cybercrimes when individuals or groups use electronic communication networks or digital platforms to spread hate speech or content that promotes enmity between different religious groups. Some cybercrimes related to Section 153A IPC can include:
(i)Spreading Hate Speech Online: Cybercriminals may use social media platforms, messaging apps, or online forums to disseminate hate speech targeting specific religious groups, promoting enmity and discord. (ii)Creating and Sharing Offensive Content: like offensive images, videos, or memes that insult or demean religious beliefs, practices, or figures, with the intent to disrupt religious harmony.
(iii)Inciting Violence: Cyber attackers may use online platforms to incite violence against a particular religious community or encourage actions that could lead to communal tensions or unrest.(iv)Manipulating Religious Narratives: Misinformation campaigns may exploit religious themes to manipulate public opinion, polarize communities, and exacerbate religious tensions.(v)Cyber Defamation[21]: Cybercriminals may post defamatory content about religious figures, institutions, or followers, causing religious tension and hurt sentiments**.(vi)**Cyberbullying and Harassment: Cyberbullies might target individuals from different religious backgrounds, subjecting them to online harassment, abuse, or threats based on their religious identity.

When individuals or groups engage in any of these cybercrimes with the intent to promote enmity or create disharmony between different religious groups, they can be charged under Section 153A IPC. Section 159 IPC pertains to "Affray. For example, if a cybercrime incident leads to widespread public outrage, heated online debates, or even threats of violence, it might contribute to an atmosphere of tension and could potentially lead to a physical altercation or an affray if people gather in public places and their disagreements escalate.

According to Sec 67A ITA 2008, Whoever publishes or transmits obscene material/-in electronic form-shall be punished on first conviction with imprisonment maximum to two three years and with fine upto to five lakh rupees and in subsequent offence imprisonment may upto to five years and with fine upto to ten lakh rupees.. Section 67 ITA does not extend to leaflet , book, drawing, painting, or figure in electronic form- to be justified as being for the public good or in the interest of science, literature, art,or learning or other objects of general concern; or which is used bona fide for religious purposes.

Manipur Fake news led to the terrifying incident, and triggered the mob to molest the women. According to police sources, the news of a rape in Delhi was spread on social media like that of a rape in Manipur which led to a mob parading and molesting two women belonging to the Kuki-Zo community.

11. Cybercrimes Offences Relating To Indian Elections

Cybercrimes in the context of offences relating to Indian elections can be committed through various means, exploiting the vulnerabilities of digital platforms and communication networks. The cybercrimes can have significant consequences for the electoral process and can include:

(i)Social Media Manipulation and Spreading Misinformation[31]: Fake accounts or bots may be deployed on social media platforms to spread propaganda, amplify certain narratives, or discredit political opponents or candidates, parties, or the electoral process. This can mislead voters and impact the outcome of elections.(ii)Phishing and Spoofing[30] Cybercriminals may engage in phishing attacks, where they send fraudulent emails, messages, or websites that appear to be from legitimate sources like election authorities. These attempts aim to steal sensitive information, such as login credentials or personal data, and compromise the electoral process.(iii)Hacking Election Systems(Sec 441IPC): Cyber attackers might attempt to breach the electronic voting machines[31] or election management systems to manipulate votes, alter results, or disrupt the electoral process or destruction of digital information through use of virus or tempering with source code. This hacking is defined in Section 66(1) read with section 43 IT Act.(iv)Denial of Service (DoS) Attacks: Cybercriminals may launch DoS attacks on election-related websites, voter registration portals, or electoral databases to render them inaccessible or disrupt the electoral process (vi)Data Breaches and Leaks[28]**:** Hackers may target political parties, candidates, or election authorities to steal sensitive data, and later use it for extortion or to manipulate public opinion**.(vii)**Election Result Tampering(Sec 65 ITA): Cybercriminals might attempt to tamper with the announcement or dissemination of election results through unauthorized access to official websites or media channels.

To counter such cybercrimes and ensure the integrity of the electoral process, election authorities and stakeholders often implement cybersecurity measures., such as:(i)Secure Voting Systems.(ii)Encryption and Secure Communication (iii)Cybersecurity Awareness Training (iv)Incident Response Plans.(v)Regular Security Audits

Election Commission of India vs. Facebook Inc.: In 2019, the Election Commission of India (ECI) filed a petition against Facebook Inc before the Delhi High Court, alleging that the social media platform was not effectively taking down content that violated Indian election laws , the Model Code of Conduct and regulations during the general elections. The Delhi High Court issued notices to Facebook Inc., seeking its response to the ECI's allegations. Section 126(1)(b) of R.P. Act 1951 prohibits display of any election matter electronic media during the period of 48 hours ending with the hour fixed for conclusion of poll.

Note Section 66(1) of ITA 2000 deals with 'Hacking'. The Representation Of People's Act 1951 Vide Section 135 A deals with offences of booth capturing. The data stored In 'EVM comes under the ambit of section 2(t) ITA 2000 tantamount to 'hacking with computer system'.

12. Cybercrimes Offences Relating To Religion

Some ways in which cybercrimes can be associated with offences relating to religion under the IPC include(i)Spreading Hate Speech: Malicious actors may use social media, messaging apps, or online forums to disseminate hate speech targeting individuals or communities based on their religion, promoting enmity and disharmony (ii)Cyber Defamation[32] :Cybercriminals might post derogatory or defamatory content about religious figures, institutions, or followers, causing religious tension and hurt sentiments (iii)Creating and Sharing Offensive Content[33]: Offenders may create and distribute offensive fake images, videos, or memes that mock or insult religious beliefs, practices, or rituals.(iv)Inciting Violence**:** Cybercriminals may use online platforms to incite violence against a particular religious group or to call for actions that could lead to communal tensions or unrest (v)Manipulating Religious Narratives: Misinformation campaigns may exploit religious themes to manipulate public opinion or polarize communities.(vi)Hacking Religious Websites or web defacement[33]: Cyber attackers might deface or hack religious websites, causing embarrassment to religious communities and disrupting access to legitimate religious content.(v)Cyberbullying(Section 66A ITA,SEC 500, 506,507 IPC) criminal intimation(Sec506 IPC) and Harassment: Cyberbullies may target individuals based on their religious identity, subjecting them to online harassment and abuse.

Some cybercrimes that can be related to Section 295A IPC include:(i)Creating and Sharing Offensive Content: Offenders may create and disseminate offensive fake[34] images, videos, or memes that insult or mock religious beliefs, practices, or figures or start violence as Manipur case.(ii)Spreading Blasphemous Material: Cybercriminals may share material that is perceived as blasphemous by a particular religious community, intending to outrage religious feelings.(iii)Defacing Religious Websites: Hackers may deface or hack religious websites, posting content that insults or defames a religion.(iv)Online Defamation of Religious Figures: Cyberbullies might engage in defamatory campaigns against religious figures, institutions, or followers, intending to outrage religious sentiments.(v)Insulting Religious Symbols: Offenders may use digital platforms to insult religious symbols, objects, or icons with the intent to hurt religious feelings. If individuals or groups are found guilty of committing cybercrimes under Section 295A IPC, they can face legal consequences, including imprisonment and fines. As per sec 79 of ITA, the service provider ISP should be liable for it, it regulate the electronic transaction and digital space and victim affected by defamatory internet posted material may bring a takedown reference.

13. Cybercrime Causing Body and Property Offences

This section comments how the cybercrimes can cause death and property loss to victim.

How the cybercrime can cause death to the victim of cybercrime?
Cybercriminals or malicious actors may spread false information related to health, safety, or emergency situations, leading to panic or the adoption of harmful practices by individuals, resulting in death or injury by hacking protected systems. Cybercrime can be a contributing factor in causing death or can result in a loss of life as below :
(i)Cyberbullying and Harassment: can lead to severe psychological distress, depression, and even suicide in extreme cases, especially in vulnerable individuals, such as teenagers.(ii)Cyberstalking[35]: Persistent and malicious cyberstalking can cause fear, anxiety, and emotional trauma, which may result in self-harm or suicide in the victim.(iii)Hacking Medical Devices[36]: In some instances, cybercriminals have targeted and hacked medical devices, such as pacemakers or insulin pumps, which can lead to life-threatening situations for the individuals dependent on these devices.
(iv)Disruption of Critical Systems: Cyberattacks on critical infrastructure, such as power grids[37] healthcare systems, or transportation networks, can have cascading effects on public safety and lead to fatalities in extreme cases: (v)Cyber Terrorism: In the context of cyber terrorism(sec66 F ITA read with sec 153A IPC) attackers may target/hack vital systems of government or cause disruptions/DOS that could endanger lives or cause fatalities. Terrorist use new technology to attack their audience by creating their violence through hacking, tampering source code, denial of service attack or create terror in the mind of the people using cyber pornography, cyber theft, , cyber spamming.

Cyber terrorism is not defined in ITA 2000. The Computer Fraud and Abuse Act 1986, USA prohibits unauthorised access to protect government computers and computer networks.(vi) spreading viruses attack by viruses on protected systems of Government: Ransomware, ILOVE YOU virus deletes files, Bubble Boy virus executed by opening email and the like. The punishment for cyber terrorism[37] is imprisonment upto life as per sec 66(F), ITA 2000.

How The Cybercrime Can Cause Offences To The Property Of The Victim Of Cybercrime?
Cyber Crime Against Property : Organized groups use the illegal trades in fake goods and mass consumption goods to generate profit by counterfeiting good and piracy due to supply and demand sides.. These types of crimes include(i) Intellectual property crimes[38] (Copyright, patent, trademark and the like) It can be describes as the copying of software, its piracy and unauthorized access and attacks on it and are controlled by Sec 66 ITA Act read with sec 66B Sec of Copy Right Act and section 120 B, 420, 468 and 471 IPC. Software Piracy- ITA applicable imprisonment may extend to 3 years or fine extend upto 5 L and offence proved under IPC, 7Years and fine.

(ii)Copyright infringement[39]: it can be described as the using of copyright materials unauthorized such as music, software, text etc. Copyright Violation-Sec 51, 68, 63A of the copy right act and Sec 415, 420IPC are applicable. The imprisonment may upto 3 years and fine upto 2 L (iii)Trademark infringement: it is a unauthorised use of a service mark or trademark or cybersquauing for using similar domain names..(iv) cyber attacks on computers[40] like Computer Assets-software, hardware and systems program such as operating systems, databases, application programs are considered as a property. These crimes include unauthorized computer hacking, transmission of viruses to damage programs/web sites/computing systems and unauthorized possession of computerized information[39] In *Satyam Vs. Siffy,* Delhi High Court is the IPR famous Case in which , Bharti Cellular Ltd. filed a case that some cyber squatters had registered domain names such as barticellular.com and bhartimobile.com with Network solutions under different fictitious names. In *The US Vs Robert Lyttle*, Cri LJ 2002, the defendant was considered guilty for hacking into governments computers and defacing government web sites.

14.Criminal Breach Of Trust (Sec 403 To 409 IPC)
To study Criminal Breach Of Trust(CBT), we will recall cybercrime causing body and property offences to relate physical criminal breach of trust- Sections 403-409 with cybercrimes as follows:

Section 403 IPC : In cybercrime cases, Section 403can be applicable when individuals unlawfully access and misappropriate digital assets, sensitive information, or funds belonging to others without their consent. For example a hacker gains unauthorized access to someone's bank account and transfers funds to their own account.
Section 404 IPC. In the context of cybercrime, A person who had access to a deceased individual's computer or digital storage devices dishonestly misappropriates valuable files or intellectual property left behind by the deceased.

Section 405IPC: Section 405 is applicable for breach of trust cybercrime cases like (i)Misappropriation of Digital Assets: Individuals or employees entrusted with access to digital assets, such as sensitive data, financial information, or intellectual property, may misappropriate or misuse these assets for personal gain or to cause harm..(ii)Unauthorized Use of Data(Sec 70 ITA): Cybercrimes like data theft or unauthorized access to confidential information often involve individuals entrusted with handling or safeguarding such data. If these individuals misuse the data for unauthorized purposes, it can be considered a criminal breach of trust.(iii)Online Financial Frauds BY Phishing (sec 66D ITA2008 Sec 379, 420 IPC): By phishing scams or advance fee fraud, perpetrators gain the trust of victims and then misuse the financial information provided by them.(iv)Breach of Confidentiality(sec 72 ITA 2000): In cybercrime cases involving the breach of confidentiality agreements, trade secrets, or non-disclosure agreements, the individuals or entities involved may be charged for the breach of trust

Section 406: Punishment for CBT: In cybercrime cases involving misappropriation of digital assets, unauthorized use of data, or financial frauds, perpetrators can be charged under Section 406 and may face imprisonment and/or fines as

per the court's discretion, the punishment for criminal breach of trust, which may extend to three years of imprisonment or a fine or both.

The offences of criminal misappropriation and criminal breach of trust find place under Section 407 to 409 deal with *aggravated forms* of criminal breach of trust.

Section 407 IPC. CBT by carrier, Clerk, or Servant: The employees, or individuals who are entrusted with handling sensitive digital information, data, or assets may be charged if they dishonestly misappropriate or misuse the property entrusted to them shall be punished for maximum 7 years in case of commission of CBT by persons entrusted with property.

Section 408 CBT by clerk or servant: In cybercrime cases, where individuals in positions of trust misuse digital assets or sensitive information, they may face stricter punishment of imprisonment of maximum to seven years with fine.

Section 409. CBT by public servant, or by banker, merchant or agent—In cybercrime cases involving public servants or individuals in a fiduciary role who misuse digital assets or sensitive information for personal gain, they may face severe penalties and shall be punished with imprisonment for life, or with imprisonment maximum to ten years, with fine.

Hacking, Data Theft case: May 29, 2021 In the case of *Jagjit Singh v. The State of Punjab*[41] {Special Leave to Appeal (Crl. No(s). 3583/2021} **,** Supreme Court of India held that apart from the ITA, 2005 a person shall also be liable under IPC, 1860 for offences such as hacking & data theft etc.

An FIR was filed On 20-10-202 by M/s TCY Learning Solutions Private Limited (Complainant-Company), under sections of IPC namely, Section 406 (Criminal Breach of Trust), Section 408 (Criminal Breach of Trust by clerk or servant in respect of property entrusted to him), Section 309 (Theft), Section 381 (Theft by clerk or servant of property in possession of master), Section 120-B and 34 and Sections 43 (damage to computer, computer-system, etc.), Section 66 (Computer-related offences), Section 66-B (dishonestly receiving stolen computer resource or communication device) of the Information Technology Act, 2000 (IT Act, 2000) about a leakage of the their software by the company's past deputy Manager and that a Company under the name of "Fourmodules.in/Fourmodules.com" was providing the software with similar look and use of the Complainant software code in the market.

15. Cheating, Personation and Trespass under IPC

Section 415 - Cheating: Section 415 could be relevant to cases where individuals are deceived or manipulated through online fraud, phishing, or other forms of digital deception. For instance, if someone is tricked into sharing their personal or financial information online, and this information is then used to commit fraudulent activities, it could potentially fall under Section 415 of the IPC.

Section 416 - Cheating by Personation: Section **416** could be relevant to cases where individuals impersonate others online for fraudulent purposes. This could include instances of identity theft, where someone uses another person's identity to deceive and commit fraud, or cases where individuals create fake profiles or personas to deceive others and gain access to sensitive information. Section 418 cheating with knowledge, **Section 419** punishment for cheating by personation and 420 cheating and dishonestly inducing delivery of property are applicable for cybercrimes.. in Sony.Sambandh.Com **Case** Investigations revealed that Arif Azim while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site. The court convicted Arif Azim under Section 418, 419 and 420 IPC.

Section 425 - Mischief: Section 425 could potentially apply to cases where individuals engage in activities that cause wrongful loss or damage to computer systems, networks, or digital data. For example, if a hacker intentionally disrupts or damages computer systems, data, or digital infrastructure, it could fall under the purview of Section 425IPC and sec 43 ITA.

Section 441 Criminal Trespass could potentially apply to cases where unauthorized individuals gain access to computer systems, networks, or online platforms with the intent to commit offenses, intimidate, insult, annoy, or cause harm. For instance, unauthorized access to someone's social media account or email account with malicious intent could be considered a form of criminal trespass.

16.Cybercrime On The Criminal Breach Of Contract Of Service

Cybercrime can impact the criminal breach of contract of service (i)Data Breaches and Theft(Sec 378 IPC Theft): Cybercriminals may target a company's databases or systems, stealing sensitive employee data, financial information, or trade secrets. (ii)Non-Performance and Service Disruptions: A cyber-attack on critical systems or IT infrastructure can cause service disruptions, preventing employees from fulfilling their contractual obligations. (iii)Contractual Obligations: A cybercrime incident could hinder an employer's ability to fulfill contractual commitments to employees, such as salary payments, benefits, or other contractual obligations. (iv)Intellectual Property Violations: Cybercriminals

may attempt to steal or misuse intellectual property owned by the employer or employees. (v)Online Fraud and Scams: Cybercriminals may impersonate an employer or create fake job offers to scam job seekers, misusing the employer's brand or reputation. This can result in damage to the employer's image and potential lawsuits for fraudulent practices.

(vi)Cyber Extortion: In some cases, cybercriminals may engage in cyber extortion, threatening to disrupt services or release sensitive information unless specific demands are met. This can create pressure on both employers and employees to breach contractual terms to avoid further harm.

According to 43 A ITAA 2006 body corporate shall be liable to pay damages for failure to protect data by way of compensation, not exceeding five crore rupees, to the person so affected. (Change vide ITAA 2008). . Sec 4 of ITA 2000 read with section 499 IPC Covers the offences of cyber defamation. Sec 65 ITA deals with tempering with computer source documents, Section 66 ITA deals with hacking with computer systems, Section 72 ITA deals with penalty for breach of confidentiality and privacy.

17. Cyber Crime- Criminal Intimation, Insult and Annoyance

Criminal Intimidation (IPC Section 503): Cybercrimes can involve threats, harassment, or intimidation made through emails, social media, messaging apps, or other online channels.

Insult and Annoyance (IPC Section 504): In the digital realm, offenders may use social media, online forums, or comments sections to insult or annoy individuals, communities, or public figures. causing unrest or disharmony. Criminal Intimidation by an Anonymous Communication (IPC Section 507): Cybercrimes can involve anonymous threats or communications sent via digital means, such as email or social media messages, causing fear or alarm to the recipients. The lack of identifiable sources can make it challenging for law enforcement to trace and apprehend the offenders.

Sending Offensive Messages through Communication Services (IPC Section 66A**):** Although Section 66A of the ITAct, 2000, was struck down by the Supreme Court in 2015, its application involved criminal penalties for sending offensive or menacing messages through electronic communication.

Section 505 public mischief. This section is applicable to cybercrimes when individuals or groups use electronic communication networks or digital platforms to make statements that could lead to public mischief, disturb public tranquility, or incite one group against another.

For cybercrimes related to Section 505 IPC, some scenarios could include[42]:
(i)Spreading Hate Speech: Cybercriminals use social media or messaging platforms to circulate statements or messages that incite one religious or ethnic group against another, promoting feelings of enmity, hatred, or ill-will.(ii)Misinformation Campaigns: Disseminating false information or rumors about a particular community or group to incite violence or create unrest.(iii)Manipulating Religious Narratives: Creating and spreading content that promotes enmity or hostility between different religious or regional communities If individuals or groups are found guilty of committing cybercrimes under Section 505 IPC, they can face legal consequences, including imprisonment and fines. In England and wales cybercrime- criminal intimation, insult and annoyance, on line harassment, stalking is protected by section 1, Protection By Harassment Act 1997

18.Attempt To Commit Cyber Offences (Sec 511 IPC)

Section 511**Of attempt to commit offences**: When it comes to cyber crimes, the attempt to commit an offense refers to situations where an individual tries to engage in illegal activities through electronic means but fails to fully execute the intended criminal act. For example, attempting to hack into a computer system(Sec 66 ITA), attempting to spread malware(Sec43(c) and 43(e) read with Sec 208), attempting to commit online fraud, attempting to launch a cyber-attack, etc., would all fall under the scope of Section 511 IPC. If a person attempts to commit a cybercrime that is punishable by imprisonment for life or a lesser term, they could be punished under Section 511 IPC. The punishment for attempting the cybercrime would be imprisonment up to half of the maximum term prescribed for the actual offense, or with a fine, or both, as stated in Section 511.

19. Conclusion

The research paper explores critical aspects of cybercrime and unravels the potential role of Indian Penal Code 1860(IPC 1860)/ Bharatiya Nyaya Sanhita 2023 (BNS 2023) in tackling cybercrimes to safeguard India's digital virtual space. The researcher present his cyber forensic experience and the diagnostic & experimentation research for the applicability of IPC 1860/ BNS 2023 in cybercrimes using various cyber court judgements and Information Technology Act 2000 and its amendments.

While the IPC provisions are not specifically tailored to cybercrimes, but it can still be relevant in certain situations involving cybercrime. The provisions of BNS 2023 apply to offence targeting a computer resource located in India, However how ? Cyber offences are neither explicitly stated in IPC Nor in BNS. The researcher identify probable IPC 1860 provisions which are also available in BNS 2023 such as (i) chapter 3 punishment IPC 1860 (ii) section 84 in

cybercrime and mental incapacity (iii) right of private defence(sec 96-106 against cybercrime (iv)chapter v of abetment (v) criminal conspiracy- section 120(vi)) cyber-crime offences against the state (vii) offenses related to the army, navy, and air force (viii) offences against the public tranquillity (ix)cybercrimes offences relating to Indian elections (x) cybercrimes offences relating to religion (xi) how the cybercrime can cause death to the victim of cybercrime? (xii) how the cybercrime can cause offences to the property of the victim of cybercrime? (xiii) criminal breach of trust (sec 403 to 409) (xiv)cheating , personation and trespass(xv) cybercrime on the criminal breach of contract of service(xvi) cybercrime criminal intimation, insult and annoyance (xvii) attempt to commit cyber offences in the context of cybercrime " Most of the chapters of "Bharatiya Nyaya Sanhita 2023" are the mirroring chapters of IPC 1860 without straightforward applicability to cybercrimes or hacking or network communication digital crimes. Therefore stake holders must be trained on the basis of guidelines for cyber-crime judgements and punishments provided by this research work.

REFERENCES

[1]. Bandu B. Meshram , Manish Kumar Singh, "Ethical Hackers' Dynamic Research Methodology And Daring Experiments", Journal of Emerging Technologies and Innovative Research (JETIR) Volume X, Issue X , July 2023 , www.jetir.org (ISSN-2349-5162):
[2]. Computer Hacking Forensic Investigator courseware volume 1, EC Council USA
[3]. Computer Hacking Forensic Investigator courseware volume 2, EC Council USA
[4]. AI being used for hacking and misinformation, top Canadian cyber official says(Updated On Jul 24, 2023):https://ciso.economictimes.indiatimes.com/news/next-gen-tech/ai-being-used-for-hacking-and-misinfo-top-canadian-cyber-official-says/102068679
[5]. Information Technology Act(ITA) 2000 , Section 66 , section 65
[6]. Thomas Babington Macaulay,(1834): https://en.wikipedia.org/wiki/Indian_Penal_Code
[7]. The Bharatiya Nyaya Sanhita, 2023(which seeks to replace IPC) :https://www.livelaw.in/top-stories/union-home-minister-states-highlights-of-bills-replacing-ipc-crpc-evidence-act-234984
[8]. The Indian Penal Code, Bare Act 2019
[9]. ITA 2000 with amendment 2008
[10]. Computer Misuse Act, 1990.
[11]. Dr. Manju Koolwal, White Collar Crimes(Indian and Abroad] , Lawmanns's New Delhi, India, 2023.
[12]. Bandu B. Meshram , Manish Kumar Singh, " Unveiling The Hackers' Methodology: Exploring Cyber Crimes, Cyber Laws And Punishment", IJRARTH00102 International Journal of Research and Analytical Reviews (IJRAR) 953, 2023 IJRAR July 2023, Volume 10, Issue 3
[13]. California Stalking Law 1990
[14]. Indian Penal Code , Supra Sec 53, 54
[15]. Malaysian Computer Crime Act 1997, Sec 3
[16]. The computer Fraud and Abuses Act USA.
[17]. B. B. Meshram, Ms. K.A. Shirsath , TCP/IP and Network Security, Shroff Publishers 7 Distributors Pvt, Ltd. Mumbai feb 2018, ISBN Number 978-93-5213-355-0
[18]. Dr. Manju Koolwal, **supra, at 256**
[19]. IPC, Supra, Sec 98.
[20]. Protection from Harassment Act 1997, sec1: prohibition on harassment, sec2 criminal offence, Sec 4 cyber violence used.
[21]. Malicious communication Act 1988, sec 1: offence to send a grossly offensive or threatening material
[22]. BBM, supra. Page at Page 483
[23]. https://en.wikipedia.org/wiki/Suhas_Katti_v._Tamil_Nadu
[24]. 2003) 71 DRJ 178 (DB): 2003 SCC OnLine Del 935,
[25]. http://supremecourtofindia.nic.in/outtoday/39511.pdf
[26]. State (N.C.T. of Delhi) v. Navjot Sandhu, AIR 2005 SC 3820.
[27]. Computer Hacking Forensic Investigator courseware Lab Manual , EC Council USA Powell, O. (2022, December)
[28]. Dr. Santosh Kumar, Cyber Laws and Crimes, Whites Mann, Publishing Company, Sept 2020
[29]. Dr. Gupta and Agarwal, Cyber Laws, Premier Publishing Company, 2023
[30]. Saurabh Trivedi, "IAF officer arrested on espionage charge",*The Hindu*", Delhi (February 09, 2018 10:26 am), available at (last visited on): https://www.thehindu.com/news/national/iaf-officer-arrested-for-espionage/article22700475.ece
[31]. Chandan Haygunde ,DRDO espionage case: Scientist files bail plea, claims info 'shared with Pak doman' was in public domain", The Indian Express Pune (August 3, 2023 03:32 IST) https://indianexpress.com/article/cities/pune/drdo-espionage-case-scientist-bail-plea-info-pakistan-woman-public-domain-8873249/
[32]. Communication Act 2003, Sec 127
[33]. Michigan Criminal Code 1993
[34]. Dr. Gupta Supra at page 1010
[35]. Elyse Samuels, How misinformation on WhatsApp led to a mob killing in India(February 21, 2020 at 3:00 a.m. EST):https://www.washingtonpost.com/politics/2020/02/21/how-misinformation-whatsapp-led-deathly-mob-lynching-india/]

[36]. Shreya Singhal v Union Of India, AIR 2015 SC 1523
[37]. Dr. Gupta Supra at page 66
[38]. Chanda, Sayantan (2022) "Data Privacy And Elections In India: Microtargeting The Unseen Collective," Indian Journal of Law and Technology: Vol. 18: Iss. 2, Article 1. Available at: https://repository.nls.ac.in/ijlt/vol18/iss2/1
[39]. William A Gorton 'Manipulating Citizens: How Political Campaigns use of Behavioural Social Science Harms Democracy' (2016) 38(1) New Political Science 61.
[40]. Michigan Criminal code 1993
[41]. B.B. Meshram Electoral Reforms In India: Socioeconomic &Legal Assessment & Evaluation, LLM Thesis, SUN, Nashik 2020
[42]. ITA Sec 77B read with IPC Sec 55
[43]. ITA, Sec 65 and IPC Sec 463,464,468, 7469)
[44]. Bandu B. Meshram , Manish Kumar Singh, Forensic For Video Tamper Detection, American Journal of Multidisciplinary Research and Development (AJMRD) www.ajmrd.com, 23 march 2023
[45]. Wayne Petherick, "Cyber stalking Obsession, Obsessional Pursuit and the digital criminal": www.criminology/stalking and The communication Act 1934, USA
[46]. Information Technology Act 2000. section 70
[47]. Company Misuse Act 1990, section 13.
[48]. Data Protection Act 1998
[49]. Copy Right Act Sec 51, 68, 63A
[50]. Computer Misuse Act 1990, USA.
[51]. Jagjit Singh v. The State of Punja[1] {Special Leave to Appeal (Crl. No(s). 3583/2021}