INTERNATIONAL JOURNAL OF EXPLORING EMERGING TRENDS IN ENGINEERING
Peer-Reviewed, Refereed, Indexed and International Journal, https://ijoeete.com/
|ISSN No. 2394-0573 |Volume: 10, Issue: 2 | July - Dec 2023

# CYBERCRIMES AGAINST WOMEN IN INDIA: LEGAL CHALLENGES AND GLOBAL COMPARISONS FOR A SAFER DIGITAL SPACE

*[1]Deepika Saini, [2]Dr. Prabhjot Kaur Ghuman*
*[1]Research Scholar, [2]Supervisor*
*[1-2] University School of Law, Department of Legal Studies, Desh Bhagat University, Mandi Gobindgarh Punjab, India*

## ABSTRACT

The rapid expansion of internet technologies has brought about significant challenges in ensuring the safety of women in digital spaces. Cybercrimes, including harassment, defamation, identity theft, and cyber pornography, disproportionately target women in India, reflecting systemic gender inequalities. Despite efforts through the Information Technology Act and amendments to the Indian Penal Code, critical gaps remain in effectively addressing these offenses. A comparative analysis with global frameworks, including those in the United States and the United Kingdom, reveals inadequacies in India's legal provisions for combating cybercrimes. This paper explores various forms of cybercrime, such as hacking, cyberstalking, defamation, and breaches of online privacy, highlighting their societal and legal implications. The study concludes that a collaborative approach involving legal reforms, public awareness, and proactive law enforcement is imperative to create a secure digital environment for women in India.

**Keywords:** Cybercrime against women, Information Technology Act, 2000, Online harassment, Cyber pornography, Cyber defamation, Cyberstalking, Legal frameworks for cybersecurity, Gender-based violence online

## 1. INTRODUCTION

The rapid advancement of technology and the proliferation of the internet have created a new realm of opportunities, but with it comes significant challenges, especially concerning the safety and security of women. In India, the digital space has opened doors for cybercrimes that specifically target women, exploiting vulnerabilities created by the internet. These crimes range from cyberstalking, harassment, defamation, and identity theft to more severe forms like cyber pornography and online trafficking. Women, who often face systemic gender-based violence in the physical world, are increasingly becoming victims of similar crimes in the virtual world. The anonymity and accessibility of the internet have emboldened perpetrators, making it easier to target women with minimal risk of accountability. Despite technological progress, the legal frameworks in India have struggled to keep pace with the evolving nature of cybercrimes. While the Information Technology Act, 2000, and its amendments have made strides in addressing certain online crimes, there remain critical gaps in effectively combating the rising instances of cyber violence against women. These challenges highlight the need for stronger, more comprehensive laws that protect women in the digital domain, recognizing that cybercrimes are not isolated incidents but a reflection of broader societal issues of gender inequality and violence.

The amalgamation of computers and diverse forms of communication comprises the digital realm. Due to the internet, the entire planet has contracted to the magnitude of a petite municipality.[1] It has enabled a limitless online realm where personal and professional engagements may thrive irrespective of geographical position. The advent of globalisation has had profound impacts on individuals' economic and cultural existences. The digital realm has been a blessing to human advancement. [2] In order to accomplish its main purpose, the Internet must unite individuals from all around the world who are inquisitive about the essential human essence that has resulted in the exploration of the digital realm. Increasingly, individuals in the 21st century are transforming into Intellect Connectors, who possess

[1] M. Dasgupta, Cyber Offence in India- An Analogous Examination, 2009, p. 1
[2] Tanaya Saha and Akanchs Srivastava, "Indian Women at Peril in the Cyber Realm: A Theoretical Framework of Causes of victimisation, International Journal of Cyber Criminology, vol. 8 No. 1, Jan.- June, 2014, pp. 57-58 accessible at: http://www.cybercrimejournal.com/ sahasrivasta vatalijcc2014vol8issue1.pdf (visited on March 6, 2017).

cognizance of the occurrences within their localities and the globe in its entirety. Their determinations are based on data that is obtainable to all, precise in the current instant, and gathered from a broad spectrum of dependable origins. Individuals are progressively cognizant of their entitlements and possibilities as a direct consequence of the uprising, and this transformative alteration can be unequivocally ascribed to the upsurge of the computer, the web, and information technology. [3] In actuality, due to globalisation in the 21st century, paper-based communication is being substituted by electronic communication as the favoured technique of correspondence between individuals worldwide.

Certain enterprises have readied themselves to shield against orchestrated cyber criminal syndicates, whereas others have not yet acknowledged this peril.[4] Technology in the knowledge epoch bestows upon us with both benefits and challenges. A greater number of individuals commenced utilising it as it provided enhanced opportunities for productivity, efficacy, and worldwide correspondence.[5] The novel platform with which humanity has been surprisingly bestowed makes no differentiation between righteousness and wickedness, virtue and vice, nation and global, moral and immoral; it solely functions as a platform for the workings of human culture. The principle of legality, in its capacity as an overseer of human behaviour, has ventured into the digital domain and is endeavouring to confront the numerous challenges presented by the online sphere.[6] Safeguarding oneself from external perils has perpetually been the sole necessity for safety and protection. By the culmination of the 20th century, 'cyberspace' had surfaced in conjunction with the conventional realm. Cybersecurity is becoming imperative to the functioning of contemporary societies as the online and offline realms become increasingly interconnected.[7] A secure virtual milieu is one wherein (and whence) behaviour is inconceivable. For a comprehensive and methodical comparison, there are several unresolved inquiries in the realm of cyber legislation.

## 2. DEFINITION OF CYBER CRIME

In spite of the exponential expansion of cybercrime worldwide, individuals employed in the field of criminal justice have been deficient in possessing sufficient and current comprehension of the ordinary truths pertaining to contemporary cyber offenders. Media depictions of cybercrime typically focus on a solitary hacker who successfully circumvents intricate safeguards and pilfers exceedingly valuable classified data. These type of offences are highly rare, yet cybercrime is regrettably prevalent.[8] More frequently than not, cyber malefactors utilise the Internet to engage in deceit, intimidation, acquire unlawful pornography, or procure pilfered music, rather than to violate the domestic or global safety of nations. Scholars have demonstrated that the United States and the United Kingdom are the two conventional superpowers providing the utmost steadfast opposition to the silicon assault. The United States possesses the utmost cyber-specific regulations, trailed by the United Kingdom, which encompasses both cyber regulations and has additionally employed conventional regulations to the intricate domains, notwithstanding the reality that British judges were initially reluctant to apply traditional law to novel computer circumstances and instead

[3] Tanaya Saha and Akanchs Srivastava, “Indian Women at Peril in the Cyber Realm: A Theoretical Framework of Causes of victimisation, International Journal of Cyber Criminology, vol. 8 No. 1, Jan.- June, 2014, pp. 57-58 accessible at: http://www.cybercrimejournal.com/ sahasrivasta vatalijcc2014vol8issue1.pdf (visited on March 6, 2017).

[4] Atul Bamara, Gajendra Singh, et.al., “Digital Intrusions and Safeguard Approaches in India: A Theoretical Evaluation of Financial Sector”, Global Journal of Cyber Offences, vol. 7 No. 2, Jan.- June, 2013, p. 49-50, accessible at : https://www.researchgate.net/publication/236682638_ Digital_Intrusions_and_Safeguard_Approaches_in_India_An_Theoretical_Evaluation_of_Financial_Sector (visited on March 6, 2017)

[5] R.C. Mishra, Cyber Offence: Influence in The New Era, 2002, p. 53

[6] Justice T. Ch. Surya Rao, “Cyber Legislation- Obstacles for the 21st Century,” Andhra Law Times, 2004, p. 24.

[7] Rutger Leukfeldt, Sander Veenstra, et.al., "Elevated Magnitude Cyber Offence and the Arrangement of the Law Enforcement: The Consequences of Two empirical Investigations in the Netherlands", Global Journal of Cyber Delinquency, vol. 7 No. 1, Jan.- June, 2013, p. 1, accessible at: http://www.cybercrimejournal.com/ Leukfeldtetal2013janijcc.pdf (visited on Oct. 19, 2014)

[8] Jose R. Agustina, “Investigating Online Offences and Delinquent Conduct”, Literary Critique of Cyber Criminology, vol. 6 No. 2, July- Dec., 2012, p. 1044, accessible at: http://www.cybercrimejournal. com/Augustinabookreview2012julyijcc.pdf (explored on March 7, 2013)

advocated for the necessity to possess a technology-specific legislation.[9] For this rationale, virtually all comparative studies employ the legal systems of these two nations. All regional establishments and State administrations have appealed for lawmakers to formulate legislation addressing cyber offences; as a result, the majority of nations have commenced doing so. Cyber offences are of contemporary inception and influence the entire planet. In this chapter, we endeavour to scrutinise the gaps and imperfections in India's cyber legislation by juxtaposing them with those of the United States and the United Kingdom. The subsequent are instances of juxtapositions:

Despite numerous authors in every nation endeavouring to elucidate the expression, the concept of "cybercrimes" remains unambiguously undefined within the legal frameworks of India, the United States of America, and the United Kingdom. The Information Technology Act of 2000, as amended in 200a, is peculiar in that it does not elucidate the term "cyber crime" or "cyber offence" or even employ this terminology. The Information Technology (Amendment) Act of 200a revised the Indian Penal Code, 1860, nevertheless the term "cyber offence" is absent in any iteration of the legislation. Scholars have diverged in their opinions regarding the precise definition of a computer offence or a computer-linked offence, as outlined in the United Nations Handbook on the Prevention and Management of Computer Associated Misconduct. There is still no universally accepted global significance of the expressions, even after numerous years. Certainly, the terms computer offence and computer-connected offence will be utilised interchangeably throughout this manual.[10] As per the handbook published by the US Department of Justice, "cybercrime" pertains to any illicit deed that necessitates proficiency in computers and associated technologies for its execution, examination, or litigation[11].

## 3. TAXONOMY OF CYBERCRIMES

The inaugural computer-enabled transgression transpired in the United States of America in 1969, coinciding with the inception of the Internet. There is no scholastic categorization of cybercrimes in the United States of America. The Computer Misuse Act of 1990 in the United Kingdom segregates computer transgressions into three categories:

1. Data and system assaults that jeopardise confidentiality, safeguard, or accessibility.
2. Offences Perpetrated Utilising a Computer
3. Offences Linked to Material

The subsequent are the cybercrimes that are explicitly mentioned in the diverse provisions of the Information Technology Act, 2000[12]. Here are a few of them:

- “Tampering with computer source documents
- Computer related offences
- Sending offensive messages through communication service
- Dishonestly receiving stolen computer resource or communication device
- Identity Theft
- Cheating by personation by using computer resource

[9] Talat Fatima, Cyber Offences, 2011, p. 453
[10] United Nations Handbook on the Avoidance and Management of Computer Associated Offence, 1994, p. 5, accessible at: http://216.55.95.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_ UN_Guide.pdf, (explored on March 15, 2017)
[11] “Computer Offence Law and Legal Explanation”, accessible at: https://definitions.uslegal. com/c/ computer-offense/, (visited on March 15, 2017)
[12] Supra note 9. p. 454

- Violation of privacy
- Cyber terrorism against the government organization
- Publishing of information, which is obscene in electronic form
- Publishing or Transmitting of Obscene Material in Electronic form
- Access protected system
- Breach of confidentiality and privacy
- Disclosure of information in breach of lawful contract
- Offences by Companies”

**3.1 Hacking or Unauthorised Access**

The global nature of the legal predicament presented by hacking in the digital realm necessitates the adoption of worldwide superior methodologies in relation to safeguarding and governance administration.[13] It's the "most excluded transgression" in a series of transgressions that progressively worsen when more individuals are harmed or more individuals are discovered to be responsible. The utilisation of penal consequences is pivotal in safeguarding and deterring wrongdoing against IT infrastructure.[14] Pursuant to the guidance of the OECD and the Council of Europe Convention, numerous countries have enacted legislation to criminalise the act of obtaining entry to another individual's data or knowledge without their explicit consent.

Section 66 previously encompassed the offence of "Hacking with Computer System" in India until it was modified by the Information Technology (Amendment) Act, 2008. Nevertheless, the phrase "hacking" has been substituted with "Computer-Associated Misdeeds." In accordance with clause 66, unauthorised access is deemed illicit solely when executed with malicious intent. Any individual who, with the cognizance that the entry they aim to obtain is unauthorised, induces a computer resource to execute a task with deceitful or deceptive intent to acquire entry is liable to a penalty of up to five million rupees or confinement for a duration that may stretch to three years, or both.

The supervisor of Vijay Bank, NIT, Faridabad, lodged a grievance with authorities regarding the case of Sanjay Kumar v. State of Haryana[15], alleging that the petitioner had been dispatched to the bank by M/S Virmati Software and Telecommunication Ltd. to uphold the software system that the company had furnished to the bank. Nevertheless, the plaintiff fabricated digital documents with the intention to deceive the accusing financial institution of interest reimbursements and inflict unwarranted harm upon the bank. Notwithstanding this, the tribunal deemed him culpable and pronounced him guilty of a transgression sanctionable under provisions 65 and 66 of the IT Act in conjunction with provisions 420, 467, 468, and 471 of the IPC, and he was handed down a period of strenuous incarceration. The petitioner appealed this directive, but the appellate court dismissed his appeal and upheld the trial court's determination.

The educational facility M/S SIS Infotech Pvt. Ltd. of Hyderabad lodged a grievance in the lawsuit State of Andhra Pradesh v. Prabhakar Sampath[16] asserting that their server had been breached and their electronic records had been extracted from unrestricted public sources. The authorities examined the occurrence, and the defendant was deemed culpable of breaching the content server of the plaintiff's establishment. He was indicted under clause 66 of the IT Act.

[13] Supra note 1, p. 52
[14] Amita Verma, Cyber Offences & Legislation, 2009, p. 65.
[15] (2013) CRR 66 (O&M) 1
[16] (2015) Academic Composition 489/2010, Hyderabad

INTERNATIONAL JOURNAL OF EXPLORING EMERGING TRENDS IN ENGINEERING
Peer-Reviewed, Refereed, Indexed and International Journal, https://ijoeete.com/
|ISSN No. 2394-0573 |Volume: 10, Issue: 2 | July - Dec 2023

'Cracking' is a federal offence in the United States, encompassed by the Computer Fraud and Misuse Act of 1986. This legislation exclusively pertains to computers possessed by the federal administration. Penal consequences exclusively pertain to an extra deed or harm in the scenario of unauthorised access to all alternative systems, such as those employed not solely by the federal government, encompassing computers harbouring national security data and computers housing financial and credit information.[17] Espionage Software Management and Confidentiality Safeguard Act, 2000 is one such Act established to avert and manage intrusion in the USA, alongside the Information Security Act, 1998, which governs the utilisation and retention of individual data or facts connected to individuals under 1030.[18]

The accused in United States v. Harris[19] was convicted of breaching the Computer Fraud and Abuse Act by unlawfully entering her employer's computer system and pilfering the Social Security Numbers of numerous individuals to employ in a deceitful credit card scheme. A gentleman from northern California who operated the most renowned "retaliation erotica" platform on the World Wide Web was condemned to 30 months in federal penitentiary on December 2, 2015, subsequent to confessing to employing another individual to breach electronic mail accounts with the intention of pilfering unclothed images that were subsequently published on his platform, as per a statement disseminated by the United States Department of Justice[20]. The United States Advocate of the Department of Justice[21] issued a statement on December 15, 2015, proclaiming the apprehension and indicting of three individuals from Florida, New Jersey, and Maryland in relation to a breaching, junk mailing, and identity misappropriation plot that aimed at the private data of 60 million individuals and generated over $ 2 million in illicit earnings.

On the contrary, the term "Hacking" is not employed in the United Kingdom, but instead falls within the encompassing expression of "unauthorised entry." The United Kingdom's Computer Misuse Act (CMA), 1990, establishes three novel unlawful transgressions in Sections 1, 2, and 3. Section 1 renders it unlawful to gain entry to computer documents without proper authorization. Secondly, if unauthorised entry to computer materials is conducted with the intention to perpetrate or facilitate the commission of future offences, then this is to be regarded as more malicious hacking or breaching. Moreover, it is illicit to modify information on a computer without authorization. Section 2 of the Severe Offence Act of 2015 introduced subsequent modifications to CMA pertaining to unauthorised access, encompassing augmenting the utmost penalty for inflicting substantial harm to human well-being or state defence to an existence behind bars, and elevating the utmost penalty for inflicting substantial harm to the financial system or the ecosystem to 14 years of incarceration. The query of whether a sanctioned user who surpasses the extent of his authorization to retrieve computer information for unauthorised purposes may be discovered. culpable of unauthorised entry was raised in the DPP v. Bignell[22] lawsuit. In a singular occurrence, two law enforcement officials unlawfully infiltrated a police database and extracted personal information for their individual purposes. The Monarch's Bench Division of the Divisional Court determined that their actions did not amount to unauthorised entry as they possessed lawful jurisdiction to limit entry to the information in question.

A computer science scholar named Lauri Love[23] was apprehended in October 2013 by the UK's National Crime Agency for transgressing the Computer Misuse Act. She was indicted for being a part of a hacking collective and for engaging in transnational data pilferage from US government systems owned by the Federal Reserve, US Armed Forces, Missile Defence Agency, and NASA. In September 2016, a British court mandated his extradition to the US

[17] Tonya L. Putnam and David D. Elliott, "Global Reactions to Cyber Offence", University of Petroleum and Energy Studies Review 1, 1999, pp. 39-40, accessible at: http://www. hoover.org/sites/default/files/uploads/documents/0817999825_35.pdf (visited on March 6, 2017)
[18] Supra note 1, p. 74
[19] (2002) 302 F 3d 72 EDNY (Second Circuit Court).
[20] United States Department of Justice, Dec. 2, 2015, accessible at: https://www.justice.gov/usao- cdca/pr/operator-revenge-porn-website-sentenced-2-years-federal-prison-email-hacking-scheme (explored on April 9, 2017)
[21] United States Department of Justice, District Court of New Jersey, Dec.15, 2015, accessible at: https://www.justice.gov/usao-nj/pr/three-men-apprehended-hacking-and-spamming-scheme-aimed-personal-data-60-million (explored on April 9, 2017)
[22] (1998) 1 Cr App R 1
[23] "Lauri Love the Scholar Accused of Breaching the US", accessible at: http://www. computerweekly.com/feature/Lauri-Love-the-scholar-accused-of-breaching-the-US (visited on April 10, 2017)

to confront hacking allegations. If found guilty, a United States court may bestow upon him a sentence of up to 99 years in prison. In this context, Indian legislation is presently quite comparable to that of the United States and the United Kingdom. Mens rea is not recognised in American jurisprudence, albeit it is acknowledged in British legislation and Indian legislation. The legislations of the United Kingdom and India both permit imputed criminal liability, whereas American law does not. In India, misconduct is solely attributed if it was perpetrated deceitfully or deceptively with the intention to cause harm.

### 3.2 Cyber Terrorism

The initial IT Act of 2000 in India did not incorporate a provision penalising the dissemination of vexatious, perturbing, vexing, or alarming electronic messages or those that aimed to promote uncertainty. On the contrary, cyber terrorism was initially explicitly tackled in the Information Technology (Amendment) Act of 2008, wherein it is defined for the first time under section 66F and the utmost punishment, lifetime incarceration, is established. With the aim to instill terror into the hearts and intellects of the populace and weaken the harmony and wholeness or safeguard of the nation, cyber terrorism is tackled in clause 1(A) of section 66 F. This segment's provision 1(B) deals with cyber terrorism that has an academic influence on the State through the pilferage or revelation of delicate information or the breach of a computing system harbouring such information. Harm to national assets and jeopardising the nation's unity both meet the criteria under Section 124 A of the Indian Penal Code.

In 2008, for example, cyber terrorism in India materialised in the shape of consecutive explosives in Ahmadabad, Delhi, Jaipur, and Bangalore. Both the 26/11 onslaught on the Taj Hotel in Mumbai in 2008 and the 2010 explosion in Varanasi left digital traces.[24] academically. To undermine national security, harmony, wholeness, and tranquilly, etc., the principal objective of cyber extremists is to acquire restricted knowledge and disseminate fear via cyber communications methods. In December of 2010, hackers known as the "Pakistani Cyber Army" infiltrated the official Central Bureau of Investigation (CBI) website. There were 117 vandalizations of governmental websites in 2011.[25] academically. During the identical duration, numerous additional pivotal NIS websites were likewise breached.

In December 2014, Mehndi Masroor Biswas[26], a distinguished Twitter advocate of the Islamic State, was indicted with cyber terrorism under section 66 F of the Information Technology Act, 2000; with promoting terrorism, enabling recruitment for terrorists, and endorsing a terrorist organisation under the Unlawful Activities (Prevention) Act, 1967; and with engaging in hostilities against India and sedition under the Indian Penal Code. As per the Indian Express, a distinctive terrorism tribunal in Bangalore concluded that there was sufficient evidence to initiate charges against him. The Computer Deception and Misuse Act was initially implemented in 1986 and has subsequently been modified twice (1994 and 1996). Assaults on the World Trade Centre and the Pentagon on September 11, 2001 incited the United States to embrace the Patriot Act, 2001, which initially delineates "cyber terrorism" and formally designates hacking as a manifestation of cyber terrorism. It asserts that anyone who intentionally and unlawfully obtains entry to a safeguarded computer or who consciously induces the transmission of any software, data, cypher, or directive to a safeguarded computer is susceptible to penal consequences.

The accused in United States v. William Sutcliffe[27] was deemed culpable of disseminating myriad social security numbers on the internet and issuing interregional menaces to cause harm or demise. The United States District Magistrate established provisions on his release, encompassing a prohibition on cybernetic utilisation and a prerequisite that he refrain from interacting with any witnesses or victims. The Twitter and YouTube accounts of U.S. Central Command were breached on January 12, 2015, by the group recognised. Be cautious, ISIS, the American fighters are approaching! Newsweek, Latin Times, and WBOC News's scholarly messaging service were all compromised by the Cyber Caliphate hacking organisation on February 10th, 201 The Newsweek Twitter account subsequently shared, "Gory Valentine's Day, # Michelle Obama! The partner, the offspring, and you are under

[24] Jyoti Rattan, Cyber Statutes & Technological Information, 2014, p. 261
[25] Ibid
[26] "In an inaugural, Pro-Islamic State Twitter Advocate to Encounter Cyber Terrorism Accusations", (Last Modified on May 13, 2016), accessible at: http://www.firstpost.com/india/in-an-inaugural-pro-islamic-state-twitter-advocate-to-face-cyber-terrorism-accusations-2779982.html (visited on April 10, 2017)
[27] United States Department of Justice (2007)

observation.[28]

In contrast to India and the United States, the United Kingdom enacted the Data Protection Act in 1984 prior to the implementation of the Terrorism Act in 2000, and in the year 1990 to regulate cyber terrorism. This legislation establishes "Terrorism" as encompassing the utilisation or menace of activity that is purposed to significantly impede or significantly disturb an electronic system designed to sway governance or instill fear in the populace or a segment of the populace. If an illicit behaviour leads to substantial detriment to human well-being or national defence, the wrongdoer could potentially encounter a lifetime of incarceration pursuant to the 2015 Legislation on Grave Offences. In April 2005, an Algerian gentleman named Kamel Boungass[29] was found guilty of contaminating the British administration. He was thought to have connections to Al-Quida. However, in the contemporary era, extremists also strive to acquire unauthorised entry to governmental computers, computer systems, and computer networks by violating the Computer Misuse Act of 1990 and the Data Protection Act of 198

### 3.3 Cyber Pornography

The Indian indecency statute was discovered in sections 292–294 of the Indian Penal Code. Prior to the IT Amendment Act of 2008, notwithstanding, the IT Act of 2000 was insufficient in its management of indecency. The Indian indecency legislation has been considerably upgraded as a consequence. After being revised, the Information Technology Act of 2000 now mandates that retaining or accessing pornographic content privately is allowable. Nevertheless, it is unlawful to disseminate or release the lascivious material. With the exclusion of Sections 67 and 67A, the Information Technology Act of 2000 forbids cyber erotica. Cyber pornography is presently subjected to the identical legal structure as conventional pornographic material due to the endeavours of sections 66 E, 67, 67A, and 67B. In the circumstance of a primary conviction for a transgression under Section 67, the wrongdoer encounters a maximum of three years in incarceration and a penalty of up to five million rupees. In the circumstance of a subsequent conviction, the wrongdoer encounters a maximum of five years in incarceration and a penalty of up to ten million rupees.

Anyone found culpable of disseminating, transmitting, or instigating the dissemination or transmission in digital format any content encompassing sexually suggestive acts or behaviour shall be penalised upon initial conviction with incarceration of either classification for a duration that may stretch up to five years and with a monetary penalty that may stretch up to ten lakh rupees, and upon subsequent convictions with incarceration of either classification for a duration that may stretch up to If proven culpable of engaging in child pornography under section 67 B, the wrongdoer encounters a maximum of seven years behind bars and a penalty of up to ten million rupees upon validation for a primary transgression, and seven years in incarceration and a fine of up to ten million rupees upon validation for a subsequent violation. The vast majority of documented cyber pornography cases in India are resolved at the judicial level. A remarkable anomaly is the instance of State of Tamil Nadu v. Suhas Katti[30], which was resolved by the expeditious inquiry carried out by the Chennai Cyber Crime Cell (CCC) in an unprecedented seven months from the date of filing the FIR. This is a groundbreaking case since it is the inaugural occasion someone in India has been found guilty of breaching Section 67 of the Information Technology Act. In this occurrence, the target experienced vexatious phone calls subsequent to becoming the focal point of defamatory, obscene, and broadly bothersome communications posted on a Yahoo chat community. She notified the offence, and following an investigation, the defendant was deemed accountable for breaching provisions 469 and 509 of the Indian Penal Code, alongside Article 67 of the Information Technology Act.

As per the scholarly examination conducted by the Gujarat High Court in the matter of Mohammed v. State[31], it has been determined that section 67 of the IT Act is not applicable to the situation involving menacing electronic communications received by the Chief Minister of Gujarat. The Juvenile Erotica Prevention Act of 1996 and the

[28] Central Bureau of Investigation, United States, accessible at: http://c.ymcdn.com/sites/www.issa.org/resource/resmgr/2015_April_CISO_Forum/Cyber_Espionage_and_Cyberter.pdf (visited on April 10, 2017)
[29] Supra note 1, p. 206.
[30] (2004) Academic Composition 4680, Egmore, accessible at: http://lawnn.com/tamil-nadu-vs-suhas-kutti/ (explored on April 5, 2017)
[31] 2010 [SCR. A/1832/2009] Gujarat.

Juvenile Internet Safeguard Act of 1998 are two anti-obscene regulations in the United States of America. The antiquated Act prohibits the deliberate production of child pornography, which is described as sexually explicit content encompassing or appearing to involve a minor, utilising any form of computer technology. Under the subsequent legislation, enterprises that offer entry to material that could potentially be detrimental to minors must undertake rational measures to authenticate the age of website visitors. Safeguarding children from encountering explicit content resulted in the enactment of the Communication Decency Act of 1996. Individuals who consciously convey indecent material for purchase or dissemination in foreign or interstate trade or via the utilisation of an interactive computer service are susceptible to an utmost term of five years in confinement for a primary violation and ten years for every subsequent violation, as per the CDA.

Despite the fact that the service provider's servers were academically located in Virginia, the accused in State v. Maxwell[32] was accused of introducing child pornography into the state because he and the victim both resided in Ohio. Notwithstanding the defendant's apparent lack of cognizance regarding the fact that the disputed communication had already traversed State borders, the defendant's consciousness was imperative pursuant to the Ohio legislation. The conviction was validated by the Ohio Supreme Court, which employed a stringent responsibility transmission criterion in its determination. A gentleman from northern California who operated the most renowned "retaliatory erotica" platform on the World Wide Web was given a 30-month term in federal penitentiary on December 2, 2015, subsequent to confessing to enlisting another individual to breach electronic mail accounts with the intention of pilfering unclothed images that were subsequently published on his website.[33] Conventional British legislation maintains that personal ownership of indecent material is not an offence if no communal endeavours are undertaken to disseminate, circulate, or showcase the substance. Nevertheless, it is academically illicit to possess or disseminate child pornographic material. Acquisition of an inappropriate depiction of a minor is an offence pursuant to Section 160 of the Criminal Justice Act, 1988.[34] In the United Kingdom, there are three academically distinct types of pornography: mild-core, intense-core, and excessive. Acquisition of exceedingly explicit material is presently a felony subject to a maximum of three years of incarceration commencing January 2009.[35]

The ownership of explicit images that portray actions endangering an individual's existence, actions causing or likely to cause severe harm to a person's rectum, chest, or reproductive organs; zoophilia; or necrophilia is considered an offence according to sections 63 to 67 of the Criminal Justice & Immigration Act, 2008. Furthermore, apart from facilitating safeguards and penalties for the perpetration of such transgressions, this legislation also excludes from its purview categorised images and so forth.

The Lewd Publications Acts of 1959 and 1964, the Telecommunications Act of 1984, and the Criminal Justice Act of 1988 are additional statutes that tackle indecency. It is presently unlawful to possess an improper depiction or simulated picture of a minor, as declared in Section 160 of the Criminal Justice Act, 1988, as amended by Section 84(4) of the Criminal Justice and Public Order Act (CJPOA), 199 The utmost penalty for this offence has escalated from three to six months in incarceration. The tribunal determined in the lawsuit of R. v. Bowden[36] that the deed of acquiring and reproducing images from the web constituted "fabricating" and was consequently sanctionable under the Statute. R v. Westgarth and Jayson[37] both presented the court with fundamentally the same predicament. The tribunal determined that the accused perpetrated an act of "creating" merely by acquiring an indecent image from the World Wide Web and exhibiting it on a computer monitor, as the indictment had demonstrated that the defendant was cognizant of the storing mechanism within his web browser application. The Federal Bureau of Investigation

[32] (2002) 95 Ohio St 3d 254 : 767 NE 2d 242
[33] Accessible at: https://www.justice.gov/usao-cdca/pr/proprietor-retribution-porn-website-sentenced-2-years-federal-detention-email-intrusion-scheme (explored on April 9, 2017).
[34] Chris Reed, Computer Jurisprudence, at 300 (2003)
[35] "Cyber Erotica", accessible at: http://www.lawyersclubindia.com/articles/Cyber-Erotica- 6396.asp (explored on April 12, 2016)
[36] (2000) 1 Scholarly Application R 438, 444.
[37] (2002) EWCA Cri 683.

apprehended Hunter Moore[38] in 2014 for operating a vengeance erotica platform where sexually explicit images were published without the agreement of the individuals involved. Moore38 and his accomplice Charles Evens were accused of colluding to commit this offence. Additionally, they were charged with conspiracy, as well as seven instances of illicitly infiltrating a safeguarded computer system to acquire data and engaging in identity theft. The Academic Justice and Courts Act of 2015 penalises the circulation of a confidential intimate image of another individual without their consent and with the intention to inflict distress upon them in the United Kingdom, thereby prohibiting retaliatory pornography. The United Kingdom Tribunal has delivered verdicts of two years and a half to Moore and two years and a month to Evens. Whilst the United States' Communication Decency Act (1994) and the United Kingdom's Obscene Publications Act (1959) establish differentiations between adult-oriented and child-oriented pornographic material, India's Indian Penal Code (IPC), as modified in 2008, does not. Nevertheless, the IT Act presently delineates child pornography as an offence and penalises it pursuant to Section 67B. Although it is not unlawful to possess indecent content in the United States, it is illicit to disseminate or transmit such material. This is not the circumstance in the United Kingdom or India. While entry to pornographic material is limited for underage individuals in the United States, engaging in such activities is deemed unlawful in India.

### 3.4 Cyber Stalking

Diverse countries possess varying regulations concerning cyber harassment. Prior to February 2013, the Information Technology Act of 2000 (IT Act) did not explicitly tackle cyberstalking. Nevertheless, provisions 66A, 72, and 72A of the IT Act accomplished the same. The Indian Parliament enacted the Criminal Law (Amendment) Act, 2013 in 2013 to render cyber harassment an offence under the Indian Penal Code, 1860. The Knowledge Technology (Amendment) Act of 2008, specifically Section 66A, and Sections 72 and 72A, do not clearly delineate cyberstalking as an offence. Transmitting indecent correspondences via a communication platform, etc., is sanctionable under Section 66 A, whereas violations of trust and confidentiality are sanctionable under Section 72.

In Shreya Singhal and others v. Union of India[39], the Supreme Court of India determined that the legislation was unconstitutional and a transgression of their entitlement to freedom of expression. Law enforcement agencies in different jurisdictions have employed this provision to unjustly apprehend individuals for articulating their viewpoints on social and political subjects on virtual platforms. Financial transgressions The department of Delhi Police registered the complaint of online harassment against Ritu Kohli under section 509 IPC for offending the decency of a woman. Harassment and stalking are both encompassed within Section 503 of the Indian Penal Code. Furthermore, there exists a resolution to the predicament of derogatory vocabulary within section 50 Cyberstalking additionally can occur when menacing or otherwise objectionable messages are received via electronic mail. Cyberstalking is illicit in the United States due to the nation's anti-stalking, calumny, and persecution legislation. Perpetrator may encounter restraining order, probation, or criminal consequences (including incarceration) if proven culpable. Recent federal legislation in the United States has incorporated provisions to counteract cyberbullying. For example, the federal interstate harassment act was modified to incorporate cyberstalking in 2000 with the enactment of the Violence Against Women Act. Nevertheless, there is still a dearth of federal legislation that specifically tackles cyber harassment, thereby permitting the majority of laws to be implemented at the state level. Certain jurisdictions have regulations against stalking and persecution that render it unlawful to dispatch someone unpleasant or menacing messages digitally.[40] Despite the fact that all fifty states implemented anti-stalking statutes subsequent to California's groundbreaking legislation in 1990, merely fourteen of them had regulations specifically addressing "cyberstalking" by 2009.[41]

Practically every US state has some sort of cyberstalking legislation. Any individual who consciously utilises the postal service, any interactive computer platform, or any means of interstate or international trade to partake in behaviour that induces significant psychological anguish to said individual or instills a rational apprehension of

[38] "Hunter Moore receives 2.5 Years for Retribution Obscenity Breaching", accessible at: https://www.cmagazineuk.com/hunter-moore-receives-25-years-for-revenge-porn-hacking/article/535569/ (explored on April 10, 2017).
[39] AERIAL 2015 SC 1523.
[40] "Digital Harassment", accessible at: http://en.wikipedia.org/wiki/cyberstalking (attended on April 12, 2016).
[41] Christa Miller, "Advanced Surveillance, Law Enforcement Technology", accessible at: http://www.officer.com/article/10233633/advanced-surveillance (explored on March 6, 2017)

mortality or severe physical harm shall be held accountable pursuant to section 2261 B (b) and may face a period of incarceration that has the potential to extend to a lifetime imprisonment in the event that the demise of the victim is a consequence of said offence. In the instance of New Jersey v. Dharun Ravi[42], a university scholar named Ravi was accused of cyber harassment after he surreptitiously recorded his flatmate partaking in suggestive behaviour with another gentleman and subsequently shared the video on the internet. She ended her life due to this conduct by Ravi, who was subsequently convicted of prejudice intimidation and breach of confidentiality. Ravi was bestowed a 30-day incarceration period and a penalty in 2012 subsequent to a court ascertaining that his deeds originated from utmost callousness rather than malevolence. A previous worker of the United States Department of Justice confessed and was indicted on December 9, 2015, in a statement released by the United States Department of Justice[43], for a global cyber harassment, electronic mail deception, computer breaching, and sexual coercion plot impacting numerous individuals in the United States.

Various forms of stalking, such as online harassment, are tackled by diverse legislations in the United Kingdom. By revising the Protection from Harassment Act (PHA) 1995 to incorporate sections 2A and 4A, the Protection of Freedoms Act, 2012 introduced two novel stalking offences. Harassing is presently a transgression under Section 2A, sanctionable by a maximum of 51 weeks in incarceration, a penalty of up to level 5 on the customary scale, or both. If you're found guilty of harassing under Section 4A and the victim is apprehensive for their well-being due to your actions, you may potentially encounter a maximum incarceration period of five years, a monetary penalty of up to twice the legal limit, or a combination of both, contingent upon the specifics of your situation. Elements of stalking as delineated by this Act encompass, but are not restricted to, the subsequent conducts: cyber surveillance; reaching out; lingering; reconnecting; tampering with possessions; and observing clandestinely. Dispatching or conveying correspondence with the purpose to induce psychological anguish or unease is an offence pursuant to the Malicious Communication Act of 1988. The Violations Against the Individuals Act (1861), the Penal Justice and Public Order Act (1994), and the Radio Telecommunication Act (2006) all tackle harassment in different manners. The conduct must be both reprehensible to the extent that it would substantiate criminal liability and tyrannical in nature, as determined by the Honourable Court in R v. Curtis[44]. The tribunal formerly determined in C v. CPS[45] that the data lodged or indictment must adequately specify things to establish the progression of behaviour amounting to harassment. Nevertheless, as stipulated in the precedent Pratt v. DPP[46], the occurrence can solely be deemed relevant if it constitutes a consistent sequence of conduct.

### 3.5 Cyber defamation

Although the term "cyber defamation" is not employed or explicitly elucidated in section 66A of India's IT Act, 2000, the action of disseminating highly derogatory material with the purpose to vex, irritate, or intimidate is deemed unlawful. Section 499 of the Indian Penal Code tackles the peril of cyber calumny, and the IT Act of 2000 broadened this provision to encompass "verbal communication" and "records" transmitted electronically. In accordance with Section 499, it is unlawful to disseminate a defamation concerning an individual if you are aware, or possess rational grounds to be aware, that the defamation would diminish that individual's standing. Slanderous remarks are disclosed, or disseminated to someone other than the intended recipient. As long as the email is not dispatched to a third party, transmitting a libellous message by email in India is not unlawful. Slanderous assertions expressed on mailing lists and the internet may reach audiences beyond the intended recipient.

The Vice President of the Delhi and District Cricket Association lodged a calumny grievance against Delhi Chief Minister Arvind Kejriwal and suspended BJP Parliament Kirti Azad on January 30, 2017, alleging that they had defamed the cricket association by employing "disgraceful" comments. Based on substantiation from an acquaintance, the Honourable tribunal deduced that "it is evidently apparent that Chief Executive, Kejriwal has made a grave libellous comment." The tribunal declared, "Such an all-encompassing declaration, emanating from the

[42] (March, 2012), SC New Jersey, accessible at: https://en.wikipedia.org/wiki/New_Jersey_v._ Dharun_Ravi (explored on April 10, 2017).
[43] Accessible at: https://www.justice.gov/opa/pr/former-us-state-department-employee-pleads-guilty- extensive-computer-intrusion-cyberharassment (explored on April 9, 2017).
[44] (2010) EWCA 123.
[45] (2008) EWHC 148.
[46] (2001) EWHC 483.

Principal Minister no more, might possess detrimental consequences and instill an unfavourable notion in the cognition of cricketers, authorities, and the populace in general, affecting the prestige of Delhi and District Cricket Association, its administrative operation, and the openness of the assortment procedure."[47] The tribunal additionally considered the reality that the aforementioned comment was transmitted globally and disseminated in all domestic publications.

One of the most advantageous tools for protecting online freedom of expression and intellectual assets in the United States is the Communications Decency Act (CDA), 1996. Any individual who consciously publishes or instigates the publication of any material on the World Wide Web that is vulgar, crude, licentious, impure, or improper with the intention to vex, mistreat, intimidate, or torment another individual is liable to incarceration and/or a monetary penalty pursuant to Section 223 of the legislation. The Act safeguards private screening and prohibiting of objectionable content under Section 230. Intellectual property providers shall not be interpreted as the publisher or orator of any data provided by any other intellectual property provider, and neither the provider nor the user of an interactive computer service will be so interpreted.

A disparaging weblog entry on a matter of societal significance cannot lead to legal recourse without substantiation of misconduct and tangible detriment, as determined by the Honourable court in the lawsuit Obsidian Finance Group, LIC v. Cox[48]. Bloggers who fabricate disparaging remarks about private individuals in public forums are solely legally accountable for their deeds if they behave carelessly. The complainant in Firth v. State of New York case[49] contended that the time limit for legal action should be prolonged because online publishing of an alleged defamation would amount to ongoing distribution. The tribunal determined that the time limit would commence on the day the material was initially uploaded, and not from the persistence. The Appellate Division of the Supreme Court of the State of New York affirmed the lower court's decision.

In the United Kingdom, the Vicious Correspondence Act of 1988 regulates the utilisation of technology to oversee electronic correspondence with grave consequences for individuals who abuse it to intimidate, menace, or torment others. It tackles cyberbullying as well, nevertheless the legislation is presently considered outdated and in require of modernization. The Defamation Act of 1996 in the United Kingdom was enacted to additionally elucidate the "unblemished propagation" safeguard for Internet Service Providers (ISPs). The Defamation Act of 1996 mandates that anyone who is not the substance's editor, publisher, or originator may possess a defence against a defamation lawsuit if specific prerequisites are fulfilled. The United Kingdom service provider must demonstrate that it took all requisite measures to evade publishing anything that may be deemed libellous. There is still the potential for legal recourse against international publications. The Defamation Act of 2013 amplifies upon preexisting defences for website operators, publications in the public interest, and publications with exceptional privileges. When a website proprietor is informed of conceivably libellous content on their site, the protocols they must undertake to evade legal accountability for the content are delineated in this legislation. The dissemination of a comment that has resulted in or is likely to result in significant harm to the standing of individuals or enterprises is deemed defamatory pursuant to this legislation. The current legislations stipulate that anyone who issues intimidations or perpetrates transgressions on digital platforms encounters a maximum of half a year behind bars and a penalty of 5,000 pounds, or both. The plaintiff in Bunt v. Tilley and Others[50] filed a lawsuit against the defendants for slander following their publication of the purportedly derogatory statements on the internet. Nevertheless, the defendants appealed for the accusations to be discarded on a synopsis basis. The query of whether or not an internet service provider (ISP) may be held accountable for content simply transmitted over their services was raised in this instance. The tribunal determined that an internet service provider (ISP) could not be deemed a publisher pursuant to customary legislation as their involvement in facilitating online publications was purely inert.

### 3.6 Phishing

Neither the primary IT Act of 2000 nor its 2008 amendment employ the term "Phishing" at any point in this

[47] "Court Summons Kejriwal, Azad in DDCA Defamation Case", Sportz Wiki, Jan. 30, 2017, accessible at: http://sportzwiki.com/cricket/court-summons-kejriwal-azad-ddca-defamation-case/ (visited on April 10, 2017).
[48] (2011) CV- 11- 57- HZ.
[49] (2000) N.Y. Court of Claims.
[50] (2006) 3 All ER 336.

stipulation. However, presently it is unlawful and liable to penalty under the Indian Penal Code and Sections 66, 66A, 66C, and 66D of the Information Technology Act of 2000. The penalty for transmitting indecent correspondences through a communication facility is delineated in Section 66 A of the Information Technology Act. If you engage in unauthorised or deceptive utilisation of someone else's digital autograph, secret code, or other distinct identifying characteristics, you shall encounter penal consequences pursuant to Section 66 C of the Information Technology Act, 2000, which was incorporated by the Amendment Act of 2008. Any occurrence of deception deception executed through the utilisation of a computer system or other communicative apparatus that is capable of, but not explicitly intended for, phishing is encompassed by Section 66 D.

The United States Federal Trade Commission initiated the inaugural lawsuit against a phisher on January 26, 200 A California teenager is alleged to have pilfered credit card data by fabricating a webpage that resembles the America Online website.[51] Subsequently, in March of 2005, Senator Patrick Leahy championed the Anti-Phishing Act in Congress, which aimed to sanction and punish the cyber offenders accountable for fabricating the deceptive websites and electronic communications. However, the ballot was thwarted. In January 2007, a California jury determined Jeffrey Brett Goodin culpable of being the inaugural cyber malefactor under the CAN- SPAM Act, 2003 for disseminating myriad unsolicited emails to AOL subscribers soliciting their credit card particulars. The CAN- SPAM Act of 2003 is the inaugural U.S. cyber legislation that establishes nationwide standards for transmitting commercial electronic mail, and it was enacted in reaction to the escalating quantity of grievances regarding unsolicited e-mails. It controlled the deluge of uninvited pornographic content and the industry for it. Every occurrence of business correspondence dispatched in contravention of the legislation bears a highest possible penalty of $ 11,000. The Deception Act, 2006 was sanctioned in England, Wales, and Northern Ireland in 2006 as a novel anti-deception legislation in the United Kingdom. On January 15, 2005, it was academically enacted. Countless individuals' entry to scamming toolkits, which are employed to generate and dispatch counterfeit electronic communications, was curtailed by this legislation. There hasn't been a decree particularly addressing phishing until present. The Act penalises deceit perpetrated through distortion, suppression, and exploitation of power. Summary conviction for deception has a maximum sentence of twelve months in jail, whereas summary indictment carries a maximum sentence of 10 years in prison.

### 3.7 Cyber Fraud

Neither the Indian Penal Code of 1860 nor the Information Technology Act of 2000 elucidate the concept of "deception" in any juridical context. The Amendment Act of 2008 incorporated a fresh Section 66 D, which specifies penalties for acts of impersonation and the utilisation of computers for deceitful intentions other than cybercrime. To transgress this stipulation is penalizable by incarceration of any kind for a duration which may stretch up to three years, and/or a monetary penalty which may stretch up to one lakh rupees, contingent on the gravity of the transgression.[52] The Premier Judicial Magistrate's Court possesses jurisdiction over this offence, may bestow bail, and can ascertain culpability or innocence. In order to prohibit and sanction computer and internet deception, the United States of America enacted the Computer Fraud and Misuse Act, 1996, which was subsequently modified in 1994, 1996, the Patriot Act, 2001, and the Identity Theft Enforcement and Compensation Act, 2008. Title 18 of the United States Criminal Code pertains to cybercrime and delineates consequences for its perpetration. For instance, transgressions of sections 1028 and 1029 of this denomination disallow deceitful activities involving social security card and credit card, as well as identity theft, respectively; sections 1341 and 1343 of this denomination disallow fraudulent activities involving mail and wire, respectively; and so forth. Title 18 U.S. Code 1030 additionally renders it unlawful to employ a computer for deceit or alternative illicit intentions. The accused in United States v. Pirello[53] published four entries on internet classified-advertising platforms to deceptively vend computers to unsuspecting purchasers. He acquired three requests in this fashion, transferred the entire payment for them into his personal bank account, but never dispatched the requested computers to the clients. Whether or whether the United States Sentencing Guidelines provision 2F1.1 (b) (3), which instructs judges to augment a sentence by two levels if the offence was executed through "mass-advertising," applied to Pirello's deceptive online advertisements was a query

[51] Jeordan Legon, “Phishing scams attract your identity”, CNN News, (Jan. 26, 2004), accessible at: http://edition.cnn.com/2003/TECH/internet/07/21/phishing.scam/index.html?iref=newssearch (explored on March 6, 2017).
[52] Section 66 D (Inserted Vide Information Technology (Amendment) Act, 2008).
[53] (2001) 255 F. 3d 728

for the court to determine. The court affirmed the lower court's ruling to enhance Pirello's sentence based on the premise that his utilisation of the online platform to solicit requests for non-existent apparatuses contravened the USSG. Segment 15 of the Larceny Act of 1968 is inept against cyber deception in the United Kingdom. In accordance with the Computer Misuse Act of 1990, an individual perpetrates a transgression if they consciously and deliberately prompt a computer to execute any operation with the intention of obtaining entry to any computer, being fully aware that such action will enable them to acquire unauthorised entry to the computer. Likewise, clause 17 asserts that entry is deemed unauthorised solely if the individual lacks the entitlement to regulate entry of the type in query to the software or information and, secondarily, if they lack the approval of any individual who does possess such an entitlement to access the type in query. In the matter of R v. Thompson[54], a computer developer for a Kuwaiti bank was charged with devising two strategies to pilfer funds from the bank by directing the company's computers to transfer money from different accounts into his personal possession. To diminish his trace, he subsequently returned to England from Kuwait, where he had relocated the funds, initiated multiple bank accounts, and dispatched a letter of solicitation to the manager of the bank in Kuwait, beseeching him to transfer the funds from his Kuwaiti account to his English bank account. Following his apprehension, he was accused of cyber deception and ultimately convicted of his digital transgressions.

### 3.8 Breach of Online Privacy

Section 66 E of the Information Technology Act, 2000 was incorporated in 2008 to furnish penal consequences for encroachments of individual confidentiality in the nation. Recording, disseminating, and transmitting visuals of an individual without their authorization infringes upon this stipulation. Any of these actions undertaken without the victim's consent are deemed unlawful under this legislation. Capturing entails the process of seizing an image employing any technological methods, encompassing yet not restricted to video recorders, cameras, closed-circuit televisions (CCTVs), a webcam on a computer, or alternative forms of electronic surveillance, like covert cameras or any variety of concealed cameras, intelligent phones, etc. The phrase "publication" pertains to the distribution of a piece in any form, be it in physical form (like a tome or journal) or electronic (like a webpage or compact disc). Transmission pertains to the process of dispatching an electronic image to another individual with the notion that they perceive it promptly, for instance, through electronic mail, the internet, real-time communication, Bluetooth, and so forth. Once the missive is dispatched, the transgression has been perpetrated in its entirety. It has no impact whether the recipient of the letter uncovers it or not. The Electronic Communications Privacy Act (ECPA) of 1986 is an intellectual wiretap act in the United States of America, and section 2511 (1) (a) of the ECPA utilises the term "anyone" to delineate the individual who instigates the breach and upon whom the liability may be imposed. The Federal Trade Commission suggested that the safeguarding of personal information online be formalised into legislation, and in 2000, the Online Privacy Protection Act was implemented to accomplish precisely that. The octet principles formulated by the Organisation for Economic Co-operation and Development to protect personal information are envisaged by the CDA in the United Kingdom.

## 4. CONCLUSION

Cybercrimes against women in India have reached alarming proportions, necessitating urgent legal reforms and societal awareness. The internet has provided a new avenue for gender-based violence, manifesting in forms like cyberstalking, harassment, defamation, and cyber pornography. Despite the existence of laws such as the Information Technology Act and the Indian Penal Code, these legal frameworks are often insufficient or inadequately enforced to fully protect women from the growing menace of online abuse. A comparative analysis of cybercrime laws globally reveals that India still has much to do in terms of refining its cyber legislation and ensuring that offenders are held accountable. The need of the hour is a more robust legal infrastructure that not only criminalizes cyber offences but also empowers women to seek justice without fear of reprisal. Addressing these issues requires collaborative efforts from law enforcement, policymakers, and the tech industry, along with educating the public about the gravity of cybercrimes against women. Only by acknowledging and tackling these crimes head-on can India create a safer digital environment where women can participate without fear of harassment or exploitation.

## REFERENCES

1. Council of Europe. (2001). *Convention on Cybercrime*. OECD Guidance on Cybersecurity.

[54] (1984) 1 WLR 962.

2. Government of India. (2000). *Information Technology Act, 2000*. Retrieved from https://www.indiacode.nic.in

3. Government of India. (2008). *Information Technology (Amendment) Act, 2008*. Retrieved from https://www.indiacode.nic.in

4. Indian Penal Code, 1860. Retrieved from https://www.indiacode.nic.in

5. United Nations. (1994). *Handbook on the Prevention and Management of Computer-Associated Misconduct*. United Nations Office on Drugs and Crime.

6. The Computer Misuse Act, 1990. (UK). Retrieved from https://www.legislation.gov.uk

7. Severe Crime and Policing Act, 2015. (UK). Retrieved from https://www.legislation.gov.uk

8. Patriot Act, 2001. (USA). Retrieved from https://www.congress.gov

9. Communication Decency Act, 1996. (USA). Retrieved from https://www.congress.gov

10. Juvenile Internet Safeguard Act, 1998. (USA). Retrieved from https://www.congress.gov

11. Supreme Court of India. (2009). *Sanjay Kumar v. State of Haryana*. Retrieved from https://indiankanoon.org

12. Supreme Court of India. (2010). *State of Andhra Pradesh v. Prabhakar Sampath*. Retrieved from https://indiankanoon.org

13. Data Protection Act, 1984. (UK). Retrieved from https://www.legislation.gov.uk

14. Defamation Act, 2013. (UK). Retrieved from https://www.legislation.gov.uk

15. Criminal Justice & Immigration Act, 2008. (UK). Retrieved from https://www.legislation.gov.uk

16. Electronic Communications Privacy Act, 1986. (USA). Retrieved from https://www.justice.gov

17. Federal Trade Commission. (2000). *Online Privacy Protection Act*. Retrieved from https://www.ftc.gov