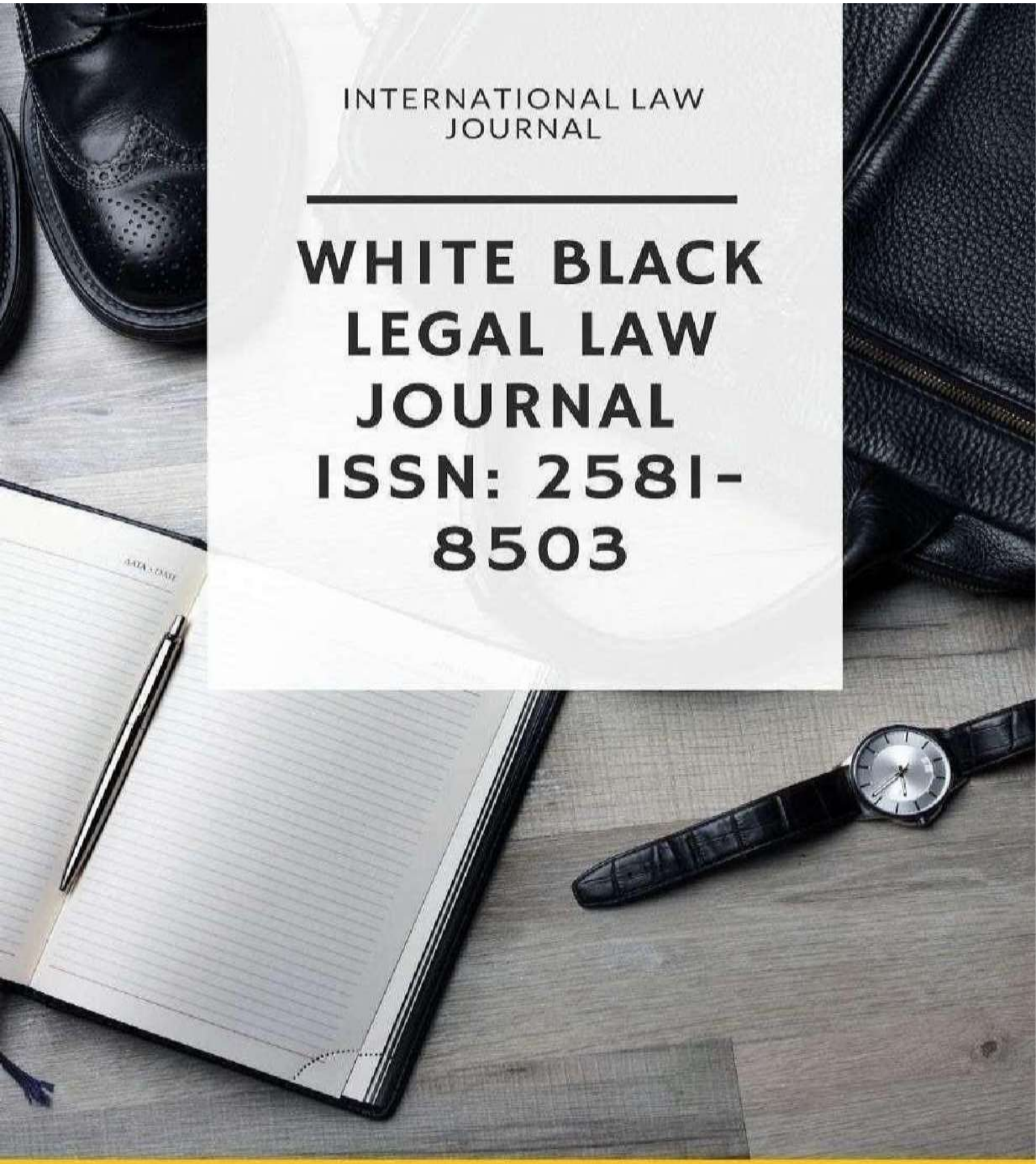

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and diploma in Public a professional Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

WOMEN CAPPED IN CYBER CRIME

AUTHORED BY - MUSKAN MITTAL,
CO-AUTHOR - SAKSHI SHARMA,
STUDENTS OF BALLB 5TH YEAR,
BABA FARID LAW COLLEGE, FARIDKOT

ABSTRACT

A catastrophe in the name of cybercrime and mobile crime spread like a virus at times when people fought against Covid-19 pandemic. There has been an increase in cyber threats taking advantage of online trends and behavior. Computers have been used by cybercriminals to gain access to private information, trade secrets or for any other malicious purposes. Offenses which are gender-specific are rising day by day, especially those related to cybercrime against women, becoming rampant in the cyber world. Cybercrime against women include sending emails which are obscene, messages through WhatsApp, cyber stalking, developing pornographic content, spoofing emails, morphing images, and many more. Though the legislations such as Indian Penal Code, 1860 and the Information Technologies Act, 2000 both attempted to some extent to prevent these offenses but the effectiveness of these laws is still up for debate. Women are mostly affected by cybercrime as they are subjected to mentally and emotional harassment. Many women face humiliation and depression which is challenging to address and resolve. Most importantly, thorough knowledge and awareness about privacy and cybercrime is the key to avoid people being vulnerable to such threats. There must be more education on cybercrime, online scamming, fraud and how to get rid of or handle them. This article throws light upon crimes committed against women becoming a part of cybercrime, legal perspective to tackle the problems faced by women and remedial measures to be taken in the form of cyber security.

KEYWORDS

Cybercrime, Women, Cyber stalking, online scam, Cyber security.

INTRODUCTION

The Internet of things is the game changer for an overall transformation of an ecosystem.

The Internet has become a living life. Each and every person spends most of his time online. With the boom in technology and an easy access to the internet across the nation, cybercrime has become a pretty common occurrence. Almost every sector in India whether it is private or government practices 'work from home' due to which hacking activities and cybercrimes are on rise particularly attacks against those using digital media for financial transactions and social media platforms at high level. Instead of making payment in cash, consumers often adopt online mode while recharging their mobile phones, paying premiums, interest loans or water and electricity bills, etc. resulting in huge amounts of loss. People easily became victims as confidential information stolen up by hackers just with a click of a button. Apart from that, the National Cyber Crime Diagnostic Centre reported there are many Over-the-top (OTT) platforms run out in India such as Netflix, Amazon Prime claiming to give discounts in large numbers. Many customers logged into it by accessing their personal information like OTP, bank account number, IFSC code, etc. to avail their services later on, fake websites marked its excel over it. A 3 month moratorium for credit card dues or EMI installments from March 1, 2020 to May 31, 2020 had been announced by RBI as SBI tweeted that 'Cyber fraudsters keep finding new ways to scam people'.[1] Phishing emails or SMS's has been send by cyber attackers to bank employees asking them for their OTP's to avail moratorium facility but truth is that EMI deferment does not require OTP sharing. Just like two sides of the same coin, there are pro and cons of technology & internet. When these disadvantages are exclusively used by a person for committing illegal acts it took the shape of cybercrime. Cybercrimes, electronic signatures, intellectual property rights, data protection and privacy are all governed by cyber laws. Moreover, the incidents of cybercrimes against women and children is also escalating. Thus, cybercrime and cyber criminals both developed at a rapid pace while law has progressed at best at a snail's pace and even that is usually only a knee jerk reaction.[2]

MEANING

In the common parlance, the term 'cyber' relates to computers, internet, or technology. thus implying that cybercrime refers to offenses committed in virtual reality with the use of the internet.

---

[1]Courtsy- Ambika Sharma & Ronit Banarjee, SBI OTP Scam: SBI warns customers against this new OTP Scam, The Times of India, Apr 9, 2020, at 1.

[2]Dawood Khan, Cyber Security Challenges In India And The Law, Legal Service India (Oct. 15, 2023, 10: 05 PM), https://www.legalserviceindia.com/legal/article-9416-cyber-security-challenges-in-india-and-the-law.html.

Cybercrime is a crime which occurs when there is any kind of illegal or unauthorized activity which takes access to your data involving use of electronic devices. Fraud, abuse as well as misuse of devices have also been included in cybercrimes. Active participation or physical presence is not necessary for the commission of cybercrime. Thus, the terminology cybercrime is not defined in any act or statute passed by the Indian Legislature and not even in Information Technology Act, 2000 but it may be interpreted judicially in some judgments passed by our Indian Courts. This is major lacuna of Information Technology Act, 2000.

HISTORICAL BACKGROUND

In 1834, the first cyber attack took place in France before the invention of internet. Financial market information has been stolen by attackers by accessing the French telegraph system. From that moment, cybercrime has been grown exponentially, marked by an intriguing evolution of tactics, techniques, and procedures — all implemented for malicious gain.[3] The exact origination of cybercrime, when someone committed a crime across a computer network, is impossible to know. What is possible to know is the first major attack on a digital network which is an evolution of cyber based crimes.[4] In 1970, an advantage was taken up by criminals of the tone mechanism employed on phone networks. It involved the attacker reversed engineering the telephone companies long distance phone calls which was known as phreaking.[5] The Computer Fraud and Abuse Act of 1986 is the first cyber law in which unauthorized access to computers and the illegal use of digital information has been prohibited. Then in 1989, the first ransomware assault was recorded which targeted the healthcare business. It was a sort of malicious software that encrypted user's data and locked it until a tiny ransom was paid. Therefore, the cybercrime developed through past occurrences.

CATEGORIZATION OF CYBERCRIME

Cybercrime has been categorized into following types:

- **Pornography of child or Non-consensual Pornography**: It is also known as cyber misuse or retribution pornography in which sexually realistic photos or recordings are

[3]Arctic Wolf, A Brief History Of Cybercrime, (Oct. 15, 2023, 10: 10 PM), https://arcticwolf.com/resources/blog/decade-of-cybercrime/.
[4]VPN Blog , Where Does Cybercrime Come From? The Origin & Evolution Of Cybercrime, (Oct.16, 2023, 10: 11), https://www.le-vpn.com/history-cyber-crime-origin-evolution/.
[5]Abhitennis, The Evolution Of Cybercrime, Legal Services India E-Journal (Oct. 8, 2023, 8: 18 PM), https://www.legalserviceindia.com/legal/article-8382-the-evolution-of-cyber-crime.html.

online dispersed without acquiesces of the person in the pictures. The offender is regularly an ex-accomplice who gets pictures or recordings over the period of an earlier relationship, and plans to openly scandal and embarrasses the person in question, in countering closure of a relationship. Photographs can also be obtained by hacking into the injured individual's computer, social media accounts or cell phone just to harm world life of victim.

➢ **Cyber stalking**: It is mode in which victims are targeted and disturbed by cyber stalkers through websites, talk rooms, dialog discussions and emails. It is not only restricted to unwanted following but repeated phone calls or sending unwarranted letters is also included in it.[6]

➢ **Defamation**: Cyber defamation involves publication of defamatory information about the person on a website or circulating it socially and among the friends circle of victims or an organization which is an easy way to ruin the reputation of women by causing her grievous mental agony and pain.

➢ **E-mail spoofing**: It is an email that emerges from one source but has been sent from another source. It can cause pecuniary damage.

➢ **Phishing**: It means to gain sensitive information such as username and password and intent to gain confidential information.

➢ **Trolling**: It is the practice where criminal starts quarreling or displeasing victim by posting inflammatory or off-topic messages in an online community (such as chat room, or blog) with the intent to provoke victims into an emotional and distressing response. Trolls are professional abusers who create a cold war atmosphere in the cyber space by creating and using fradulent ids on communal media and they are difficult to trace.

➢ **Cyber flirting:** Generally, it is considered a very minimal petty offence where victim is forced by perpetrator to hear obscene music, messages resulting in cyber sexual defamation and breach of thrust.

[6]Varalika Nigam, India: Cyber stalking and The Indian Jurisprudence, Mondaq (Oct. 8, 2023, 8: 18 PM), https://www.mondaq.com/india/social-media/1193320/cyberstalking-and-the-indian-jurisprudence.

➢ **Cyber Harassment**: It is a dreary conduct of harassing a person online by the medium of the internet. A specific class of pestering which is sexual in nature is known as sexual harassment. Under Indian law a physical contact and advances including unwelcome and express sexual suggestions is included in sexual harassment as added by Criminal Law Amendment (Bill) 2013.[7]

➢ **Theft of Data**: The term 'data theft' is used to depict when information is unlawfully replicated or taken from a business or some other person. Generally, this information is related to the client, for instance, passwords, social security numbers, Visa information, personal information, or other private corporate information.

CYBER CRIME LAWS IN INDIA

There are a number of laws in terms of cyber security that administer the use of cyberspace and supervise the use of information, software, electronic commerce, and financial transactions in the digital world. Indian cyber laws have enabled electronic commerce and electronic governance to flourish in India by safeguarding maximum connectivity and minimizing security protocols.[8]

1. **The Information Technology Act, 2000**: It is the India's first-ever landmark cybersecurity law enacted by the Parliament of India and administered by the Indian Computer Emergency Response Team (CERT-In) to guide Indian cybersecurity legislation, institute data protection policies, and govern cybercrime. It also protects e-governance, e-banking, e-commerce, and the private sector, among many others. However, the Act was amended in the year 2008 which prescribed the definition and punishment of cyber crime.[9]

a) Section 43 of IT Act, 2000 - Where the computer is damaged without the owner's consent then the owner is fully entitled to refund for the complete damage.

b) Section 66 of IT Act, 2000 - Any conduct described in Section 43 that is dishonest or fraudulent punishable with three years of imprisonment or a fine of up to Rs. 5 lakh.

---

[7]Yamini, Criminal Law (Amendment) Act, 2013: Sexual Offences, Lawctopus, (Oct. 15, 2023, 11: 16 AM), https://www-lawctopus-com.cdn.ampproject.org/v/s/www.lawctopus.com/academike/criminal-law-amendment/?

[8]Nikunj Arora, Cyber crime laws in India, Blog Ipleaders, (Oct. 16, 2023, 8: 36 PM), https://blog.ipleaders.in/cyber-crime-laws-in-india/.

[9]Id. at 6.

c) Section 66B of IT Act, 2000 - Where stolen communication devices or computer is received fraudulently punishable with an imprisonment of three-year & a fine of up to Rs. 1 lakh.
d) Section 66C of IT Act, 2000 - Theft of digital signatures, password hacking, and any other forms imposes imprisonment up to three years along with Rs. 1 lakh as a fine.
e) Section 66D of IT Act, 2000 - Cheating by personating using computer resources punishable with an imprisonment of up to three years and/or up-to Rs 1 lakh fine.
f) Section 66E of IT Act, 2000 - Where pictutes of private areas are taken, published or transmitted without a person's consent is punishable with an imprisonment of up to three years and/or up-to Rs 2 lakh fine.
g) Section 66F of IT Act, 2000 - An individual who is convicted of a crime of cyber terrorism can face imprisonment of up to life.
h) Section 67 of IT Act, 2000 - In case of electronically publishing if person is convicted then he has to undergone the prison up to five years and the fine is up to Rs 10 lakh.

2. **The Indian Penal Code, 1860 (IPC):** Where the IT Act is not sufficient to cover specific cybercrimes, then IPC sections will be applicable by law enforcement agencies. Before 2013, there was no regulation that directly deals with cyber bullying or online commission of crimes against women. Sections 354A to 354D are added to the Indian Penal Code, 1860 by the Criminal Amendment Act 2013.[10]

   Section 354D deals with prohibition of online stalking. When a woman is approached or pursued by a man despite the woman's obvious disinterest in the interaction, or when online behavior of woman, use of internet, or electronic communication is observed by a guy it took shape of stalking. If found guilty of stalking, a man might spend up to three years in jail and a fine, and on subsequent convictions could land him in prison for up to five years and a fine. In addition to the specific amendments to the Code, there are a number of other provisions that deal with reporting of cyber-attacks and the prosecution of those who are responsible.[11]

[10]Parth, Cyber Crimes against Women, Legal Service (Aug. 24, 2023, 9: 40 PM), https://www.legalserviceindia.com/legal/article-8918-cyber-crimes-against-women.html.
[11]Id. at 5.

JUDICIAL PRONOUNCEMENTS ON CYBER CRIMES

1. **Manish Kathuria v. Ritu Kohli, (2018)**

   Ritu Kohli Case was the first case of India related to cyber stalking where Ritu Kohli griped to police against a person, who was utilizing her personality to visit over the Internet at the website in Delhi channel for four sequential days.[12] Thus, search was made by police and the guilty party was captured. A case was registered under section 509, of Indian Penal Code, 1860 (IPC) and he was discharged on safeguard.

2. **State of Tamil Nadu v. Suhas Katti, (2004)**

   In this case, the denounced Katti posted yahoo messages that are foul and slanderous about a separated lady requesting her for sex. He was indicted under section 469, 509 of Indian Penal Code, 1860 (IPC) and 67 of the Information Technology Act 2000 (IT) and was detained and charged with fine for a long time.[13]

3. **Dr. L. Prakash v. Superintendent**[14]

   In this case, a woman was constrained by an orthopedic specialist to perform sexual acts and later on transfer and deal these recordings as grown-up stimulation materials worldwide. He was charged under section 506 (which endorses discipline for terrorizing of criminal to cause death or hurt unfortunately), 367 (which manage grabbing or kidnapping for causing death or appalling hurt) and 120-B (criminal intrigue) of the IPC and Section 67 of Information Technology Act, 2000 (which manages offensive distribution in the internet).[15] He was condemned to forever detainment and a monetary fine of Rs. 1, 25,000 under the Immoral Trafficking (Prevention) Act, 1956.

4. **Avinash Bajaj v. State (N.C.T) of Delhi**[16]

   The famous Bazee.com case, the CEO Avinash Bajaj was arrested for an advertisement by a user to sell the DPS sex scandal video. The video was not uploaded on the portal, despite that, Avinash was captured under Section 67 of The Information Technology Act.

---

[12]Shyamapada Ghorai, (Dr.) N. K. Thapak, Study on the Case Laws Registered Regarding Cyber Crime against Women, i-publisher (Aug. 26, 2023, 9: 36 PM), http://ignited.in/a/58442#.
[13]Id. at 3.
[14]Dr. L. Prakash v. Superintendent, (2008) 3 MLJ (Crl) 578.
[15]Shyamapada Ghorai, (Dr.) N. K. Thapak, Study on the Case Laws Registered Regarding Cyber Crime against Women, i-publisher, (Aug. 26, 2023, 9: 36 PM), http://ignited.in/a/58442#.
[16]Avnish Bajaj vs State (N.C.T.) Of Delhi, (2005) 3 CompLJ 364.

Subsequently, in 2011 the Intermediary guidelines were passed whereby liability of an intermediary would be absolved if due diligence is exercised by them to ensure obscene content is not displayed on their portal.[17] The bail is granted to Mr. Bajaj subject to furnishing two sureties of Rs.1 lakh each and he was ordered by court to surrender his passport and not to leave India without the permission of the court. The Court also ordered Mr. Bajaj to participate and aid in the investigation.[18]

5. **Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank, (2018)[19]**

Rajesh Aggarwal of the IT department of Maharashtra ordered Punjab National Bank to pay Rs. 45 lakh to Manmohan Singh Matharu, MD of Pune-based firm Poona Auto Ancillaries.[20] In this case, Rs 80.10 lakh was transferred by a fraudster from Matharu's account at PNB after the latter answered a phishing email. By responding to the phishing mail, the complainant was asked to share the liability. Thus, the bank was found negligent because there were no security checks conducted against fraudulent accounts opened to defraud the Complainant.

6. **Kalandi Charan Lenka v. the State of Odisha[21]**

Where obscene messages from an unknown number received by the victim which has damaged her reputation. Emails and a fake account on Face book containing morphed images of her have been created by the accused. Therefore, the accused is found prima facie guilty of cyber stalking by the Hon'ble High Court on various charges under the IT Act and Section 354D of IPC.[22]

7. **SMC Pneumatics (India) Pvt. Ltd v. Jogesh Kwatra, (2014)**

In this case defamatory and obscene e-mails about its Managing Director was sent by an employee of company just to degrade the goodwill of plaintiff company The defendant

[17]Dr. Sanyogita & Anjali Singh, Role of Judiciary in Curbing Cybercrimes against Women and Children in India, 9, Commonwealth Law Review Journal, 206, 215 (2023).
[18]Garima Tiwari, Understanding Laws: Cyber Laws and Cyber Crimes, LexisNexis, Oct. 15, 2023, 8: 25 PM), https://store.lexisnexis.in/understanding-laws-cyber-laws-and-cyber-crimes?.
[19]Prerana Rudra, Critical Analysis on Right to Privacy, Legal Service India (Aug. 25, 2023, 8: 31 PM), https://www.legalserviceindia.com/legal/article-9569-critical-analysis-on-right-to-privacy.html.
[20]Nikunj Arora, Cyber crime laws in India, Blog Ipleaders, (Oct. 16, 2023, 8: 36 PM), https://blog.ipleaders.in/cyber-crime-laws-in-india/.
[21]Kalandi Charan Lenka v. State of Odisha, (2017) 52 SCC, 1.
[22]Nikunj Arora, Cyber crime laws in India, Blog Ipleaders, (Oct. 16, 2023, 8: 36 PM), https://blog.ipleaders.in/cyber-crime-laws-in-india/.

was identified by the plaintiff with the help of a private computer expert and moved to the Delhi High Court. An ad- interim injunction granted by Court and the employee is restrained from sending, publishing and transmitting e- mails, which are defamatory or derogatory to the plaintiffs.

CYBER CRIMES AFFECTING THE WOMEN

Cybercrime against women is at a disquieting stage and it might act like a noteworthy threat to the security and safety of a person. Every second, one woman in India gets tricked to be a victim of cybercrimes as online platform is now become the new podium where a woman's dignity, privacy and security are increasingly being challenged at every moment. Trolling, abusing, threatening, stalking, voyeurism, body-shaming, defaming, surveillance, revenge porn are forms where women is indecently represented. In cybercrimes against women, there is more mental effect than physical while the focus of the laws ensuring security of women is more on physical than mental hurt. It is factual that the National Crime Records Bureau (NCRB) of India does not maintain any separate record of cybercrimes against women. Technology is the resource used by some perpetrators who target to defame women by sending obscene WhatsApp messages, e-mail, stalking of women by using chat rooms, websites, and worst of all by developing pornographic videos, mostly created without their assent, spoofing e-mails, morphing of images for pornographic content by using various softwares available online. Women still do not go to the police agencies to complaint against sexual harassment, regardless of whether it is real or the virtual world they are likely to avoid off the issue as they feel that it might harm their family unit.[23]

Indian women are not able to report cybercrimes against them immediately as they are not really aware as where to report such crimes or are not that serious about reporting the same due to embarrassment and orthodox thinking of the society. Their mind-set needs to be broaden and they must be the whip to curb down by taking derring-do against such perpetrators *i.e.* to go ahead and lodge an immediate complaint. Most of the problems can be solved if the crime reported by women immediately and abuser is warned about taking strong legal action. Ordinarily, cybercrimes incepted through fake ids created on Facebook, Twitter and other social media platforms causing grave harm to women, as through these platforms, major blackmailing, threatening, bullying, or cheating via messages on social networking and emails are done by the perpetrators. These cyber-crimes perpetrated by men with mala fide intention such as illegal gain, revenge, insult to the

[23]Agencies, India emerging as major cybercrime centre: Study, The Indian Express, Aug. 5, 2023, at 3.

modesty of a woman, extortion, blackmailing, sexual abuse, defamation, incite hate against the community, prank satisfaction of gaining control and to steal informational content. Some of the major well-known cybercrimes have put thousands of women into various health issues such as depression, hypertension and has been suffered from anxiety, heart diseases, diabetic and thyroid ailments due to electronic harassment.

RECENT SCENARIO

In the name of Information Technology Rules, 2011, the most significant amendments were made which include provisions for the regulation of intermediaries, updated penalties and violation fees for cybercrime, cheating, slander, and nonconsensual publishing of private images, as well as censoring or restriction of certain speech.

In 2020, as per the report of The National Crime Records Bureau (NCRB) in its publication "Crime in India", a total of 305 and 1102 cases of cybercrime against children were registered during the year 2019 and 2020 respectively and the cybercrimes against women have been registered as 8379 and 10405 for publishing and transmitting sexually explicit content where the complainants or victims are women or juveniles between the ages of 12 and 17 years.[24]

Nowadays, women are made a fundamental target on social media platforms. Female activists who voice their personal beliefs have come under attack from their adversaries. The National Cyber Security Strategy of 2020 was the long-awaited follow-up plan by the government of India to further improve cybersecurity efforts. It's main goal is to serve as the official guidance for stakeholders, policymakers, and corporate leaders to prevent cyber incidents, cyber terrorism, and espionage in cyberspace.

In 2021, cybersecurity incidents involved the incidents that revolved around unauthorized access and compromised personal data. For instance, in the case of Air India, data files from more than 4.5 million customers were leaked in a cyber attack. In a separate incident, personal data leaks of around 180 million users were straightly stolen from the database of Domino's India.[25] In January 2021, it was denied by centre that there was a data leakage of 150 million Indian and put forth into

[24]ANI, 11% jump in cyber crime in 2020, NCRB data in Home Panel report, Business Standard, Sept. 25, 2023, at 1.
[25]ET Online, Air India sued over data breach, flyer seeks Rs 30 lakh in damages, ET The Economic Times, July 07, 2021, at 1.

sale. The matter was looked into by CERT-IN with the help of other international IT experts who was informed to the public at large by the IT Minister.[26]

A report on crimes against women was released by the Delhi Commission for Women (DCW), Chief Swati Maliwal in the National Capital last year in 2022 which showcases the data of six lakh calls received by her on its helpline 181 regarding 5800 complaints of rape and sexual harassment while 38,000 complaints of domestic violence in Delhi.[27] In the case of email harassment also cyber stalking is not often secured by the current cyber laws in India. It is secured just under the ambit of Section 72 of the IT Act that culprits can be remotely reserved for rupture of classification and privacy. The charge may likewise be reserved under Section 441 of the IPC for criminal trespass and Section 509 of the IPC again to shock the humiliation faced by women.

Moreover, in 2022, The IBM Security Data Breach Report states that for the fiscal year of 2022, the average data breach costs in India have reached to ₹17.5 crores (₹175 million) rupees, or around $2.2 million, which is an increase of 6.6% from 2021, and a staggering 25% from the average cost of ₹14 crores in 2020.[28]

In 2023, the Indian Central Government passed its long-awaited Digital Personal Data Protection Act (DPDP). This act borrows its broad definition of personal data from the EU's General Data Protection Regulation (GDPR) with the aim to protect data principals and restrict the activities of data fiduciaries. The petitions received in this cell are forwarding to the concerned Police Station for initiating legal action. Cyber Cell provides all necessary assistance to the Investigating Officers for collecting digital evidences.

WORKING OF CYBER CELL DEPARTMENT

Many cyber cells have been established by the crime investigation team in different cities of India,

[26]Akankhya Kabi, Dr. A. Marisport, Dr. Saira Gori, Dr. Anjani Singh Tomar, The Facets Of Cyber Crimes Against Women In India: Issues And Challenges, Vol. 6, No. 8, Journal of Positive School Psychology, 10220, 10220 (2022).
[27]Snehashish Roy, Delhi women helpline received 6.30 lakh calls in a year; domestic abuse among top cases, HT, Sept. 25, 2023, at 1.
[28]Lakshmi Visakha K B, IBM Report: Average cost of a data breach in India touched INR 179 million in 2023, IBM (Oct. 15, 2023, 7: 55 PM), https://in.newsroom.ibm.com/IBM-Report-Average-cost-of-a-data-breach-in-India-touched-INR-179-million-in-2023.

to take care of the reports and investigations of the cybercrimes. Cyber Cell is functioning in District Police Head Quarters. Complaint of cybercrime in written form anytime made to the cyber police or crime investigation department i.e cybercrime cell either offline or online mode of any jurisdiction. As per the Information Technology (IT) Act, a cybercrime comes under the purview of global jurisdiction which means that complaint of cybercrime can be registered with any of the cyber cells in India, irrespective of the place where it was originally committed or the place where the victim is currently residing or staying.[29] In the written complaint, name, contact details, and address for mailing must be provided by addressing the written complaint to the Head of the cybercrime cell of the city where the cybercrime complaint has been filed.

First Information Report (FIR) at the local police station can be filed in case not having access to any of the cyber cells in India. The Commissioner or the Judicial Magistrate of the city can be approached in case complaint is not accepted. The victim can even file a cybercrime complaint at the online portal https://cyber crime.gov.in/Accept.aspx, which is an initiative of Government of India that caters to complaints pertaining to the online Child Pornography (CP), Child Sexual Abuse Material (CSAM) or sexually explicit content such as Rape or Gang Rape (CP/RGR) content and other cybercrimes such as crimes committed through social media, online financial frauds, ransomware, hacking, cryptocurrency crimes, and online cyber trafficking. An anonymous complaint about reporting Child Pornography (CP) or sexually explicit content such as Rape/Gang Rape (RGR) content can also provided at the portal.

In Punjab, cybercrime cell named as Cyber Crime Police Station DSP cybercrime located at S.A.S Nagar, Patiala, Punjab. Cyber cell is not endowed with the investigation of cases or enquiry of petitions directly. In addition to the day to day routine work, awareness to be conducted by the officials of Cyber Cell in the school and college students with a view to educate the new generation about the forecoming threats from cyber space and also about the Cyber laws like Information Technology Act 2008 and to educate them about developing good morality in using networks electronically.

EFFECTIVE INVESTIGATION TECHNIQUES

The most common cybercrime investigation tools used by investigators are the following: -

[29]What is Cyber Crime in India & How to File Cyber Crime Complaints?, MYADVO (Sep 12, 2019), https://www-myadvo-in.cdn.ampproject.org/v/s/www.myadvo.in/blog/how-to-file-a-cyber-crime-complaint-with-cyber-cell-in-india/amp/?.

1. **Digital Forensics Software**:- Popular digital forensics software includes tools like EnCase, FTK, and Autopsy. It helps to recover deleted files and examine network traffic logs.

2. **Network Analysis Tools** :- It helps in identification of suspicious activity and tracking of the flow of data. It involves tools like Netscout, Wireshark etc.

3. **Password Recovery Tools** :- It helps in recovering databases and passwords from encrypted files. The tools such as Cain and Abel, John and Ripper etc. are included in it.

4. **Social Media Analysis Tools** :- They are used to track activities of suspects and gathering of evidence from social media platforms. Tools such as Hootsuite, Followerwonk, and Mention etc. are included in it.

These are just a few instances of the many cybercrime investigation tools available to investigators. It is important for investigators to have a deep understanding of these tools, as well as knowledge of the latest trends and techniques in cybercrime investigation.[30] By using these tools effectively, investigators can help to identify and prosecute cyber criminals and protect individuals and organizations from the growing threat of cybercrime.

CRITICAL ANALYSIS

The India's Cybersecurity Laws and Regulations have been critically analysed. One of the main hurdle with India's regulations in the cybersecurity landscape is that the government still prosecutes under unclear or outdated statutes, by which progress and the implementation of adequate cyber laws and regulations can be hindered. It creates a difficulty for organizations to derive proper guidelines and advisories from ambiguous laws and fragmented legislative approaches in privacy of data and cybersecurity.

Cybersecurity standards that have been widely accepted are more comprehensive and informative cybersecurity laws must be passed by India for its maintainability and clarified regulations and reforms to develop a better cybersecurity framework and data protection legislation. Otherwise,

[30]Esteban Borges, Cyber Crime Investigation Tools and Techniques Explained (Aug. 19, 2021), https://securitytrails.com/blog/cyber-crime-investigation.

the government of India, its law enforcement agencies, and designated regulators remain bound to follow old laws, which may result in addressing and resolving cybersecurity issues improperly.

In 2021, special petition was filed where it was ruled by Supreme Court that cyber attacks and theft of data are a crime under the Information Technology Act 2000 (IT) and the Indian Penal Code, 1860 (IPC). Since the IPC criminal statute is over 150 years old, a more modernistic and renewed IT Act of 2000 is the main regulation against cybercrime as of today. However, more work and amendments are required to revise errors and further clarification to be provided in response to new, emerging threats of the modern-day times.

REMEDIAL MEASURES TAKEN UP BY INDIAN GOVERNMENT

'Police' and 'Public Order' are subjects of State as per the Seventh Schedule of the Constitution of India. The States or Union Territories (UTs) are primarily responsible for the preventing, detecting, investigating, and prosecution of crimes including cybercrime through their Law Enforcement Agencies (LEAs). The initiatives of the State Governments have been supplemented by the Central Government through advisories and financial assistance under various schemes for their capacity building. To brace the mechanism to curb the menace and to ensure safety and security of women and young children on online platforms in a comprehensive and coordinated manner, the following measures have been taken by the Central Government in consultation with various stakeholders:

a) The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[31] empower the users of Intermediaries to adopt a robust grievance redressal apparatus including time-bound disposal of grievances. The communication to users not to host, display, upload, modify, circulate, transmit, update or share any information that is inter alia detrimental, defamatory, obscene, invasive of privacy of another, harm minors in any way or are otherwise against the law. The Indian Cyber Crime Coordination Centre has been established by the Government under the Ministry of Home Affairs that provides for a framework and ecosystem for LEAs to cope up with the cyber crimes in a comprehensive and coordinated manner.

[31]Smt. Smriti Zubin Irani, Online Cyber Grooming of Women and Young Children, PIB Delhi (Oct. 15, 2023, 7: 55 PM), https://pib.gov.in/Pressreleaseshare.aspx?PRID=1806602.

b) Under the Nirbhaya Fund, a project is implemented by the Government in the name of 'Cyber Crime Prevention against Women and Children (CCPWC)', through which steps are undertaken for spreading wakefulness about cybercrimes such as issuance of alerts or advisories, capacity building or training of law enforcement personnel or prosecutors or judicial officers, improving cyber forensic facilities and so on.

c) A National Cyber Crime Reporting Portal (www.cybercrime.gov.in) has been launched to enable the public at large to report incidents of cybercrimes focusing especially on cybercrimes against women and children.[32]

d) A toll free number 1930 has been launched for providing an assistance in lodging cyber complaints online.

e) In 2017, guidelines were issued by the Central Board of Secondary Education (CBSE) to schools on the safe and secure use of the Internet.

f) Awareness has been created by MeitY in the name of Information Security Education & Awareness (ISEA) Programme among users including women and children highlighting the essence of digital safety while using the Internet.

CONCLUSION & SUGGESTIONS

The expanding reliance on technology in our daily lives has made an unparalleled open doors for criminal actions and abuse. The Internet has become a tool of evil deeds that has been exploited by intelligent people for evil motives. Creation of phony and fraudulent profiles, cyber bullying, and online stalking tends to be one of the biggest challenges. It has been extremely difficult territory to deal with cyber space due to which some activities have been classified as gray activities that cannot be governed by law. There is absolutely no complete law on cybercrime anywhere in the arena. In India as well as across the globe there is need for constant up-gradation and refinement in cyber laws to keep pace. However, it depends on the users to participate in the fight against cybercrime. The helplessness and insecure environment for women is one of the greatest worries of any criminal and penal law, however lamentably women are still not protected in cyberspace. Following are some of the suggestions to look forward for :

- Media and Press should exercise its responsibility by creating consciousness among people regarding cybercrime.

[32]Id at 2.

- The lawmakers, internet providers, banks, shopping websites and other intercessors should work together to prevent the menace of cybercrime. To counter cybercrime against women in India, strict changes in penal code are required.
- The Union must implement strict deterrence policies and cyber security reforms to protect India's strategic, sovereign, economic and commercial interests in cyberspace.
- Do not reveal your passwords to anyone. Keep your passwords confidential and complicated.
- Do not leave your webcam connected. There are many apps which turn on your camera icon and catch-up your movements without your knowledge. So, disable permission for camera and keep your lens of camera shut off or covered when not in use.
- Do not share more than necessary information even to close relations. There are two shades in a spectrum of relationship – very good or very bad. Even the best of people can dangle from one end of the spectrum to the other.
- Do not meet online connections alone. Always let your friends and family know where you are going and whom you are meeting. Make sure the person you meet in a crowded place.
- Be vigilant about posting details about your whereabouts and lifestyle. Stalkers can easily find ways to reach you with a simple snap or status update.
- Remember to update all operating systems on your devices timely. Having a cell phone or a tablet without a security structure in place is like sitting in a house with the doors unlocked.
- Know and carefully understand the privacy policy and terms of service you use.
- The procedure for reporting cybercrimes is more or less the same as for reporting any other kind of offence. The local police stations can be approached for filing complaints just as the cybercrime cells are designated with the jurisdiction to register complaint. Additionally, provisions of 'e-FIR' has been made in some states. Every police station must have expert-trained police officials to deal with cybercrime complaints. If a police official refuses to register the complaint, a representation can be given to the commissioner of police or the superintendent of police. If action is not yet taken, then either the private complaint could be lodged before the concerned court or a writ before the concerned High court.

'Cybercrime is the gateway to jail; Cyber safety is the system to avail'