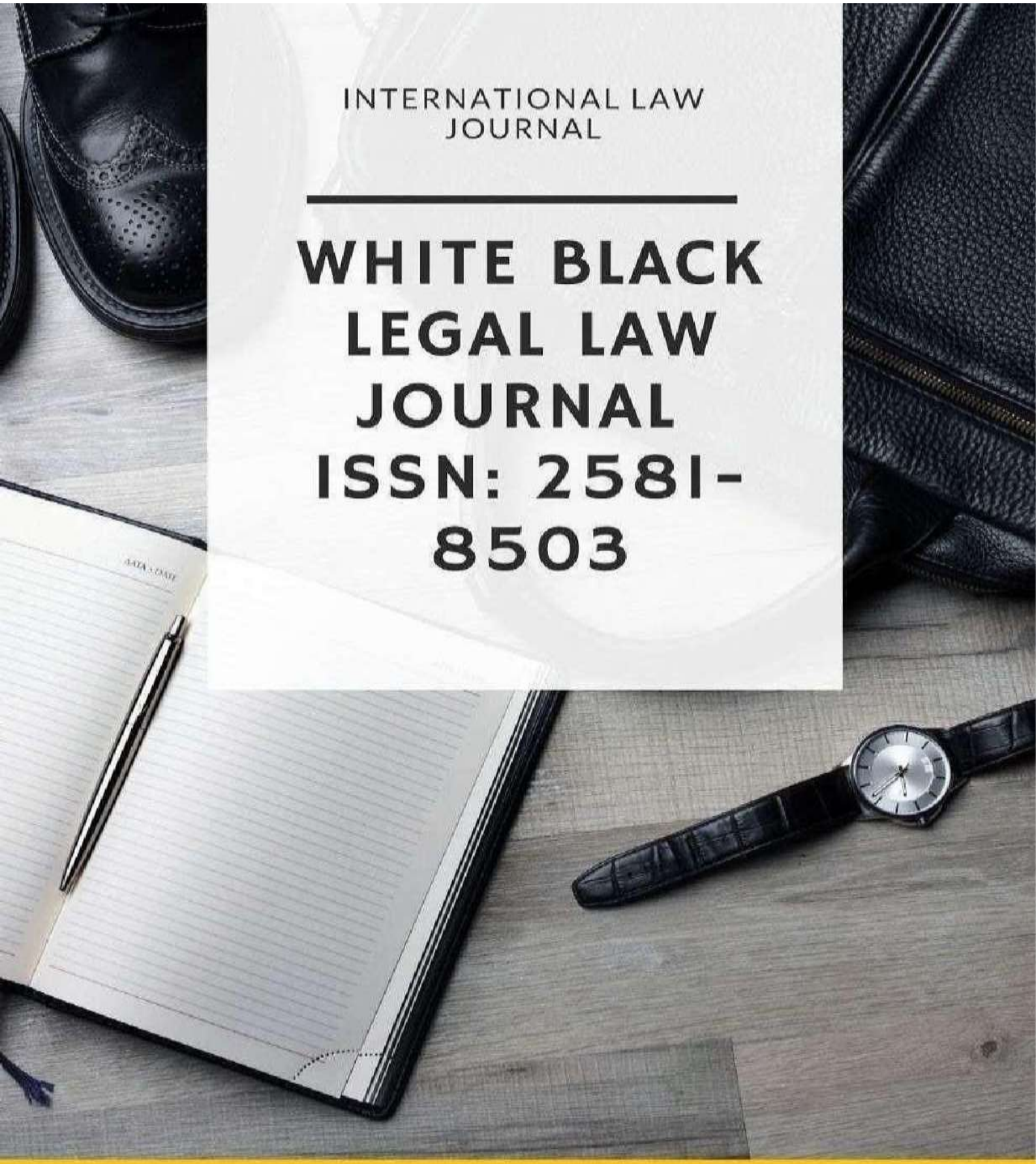

INTERNATIONAL LAW JOURNAL

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

DISRUPTING STEREOTYPES: AN INVESTIGATION OF THE MOTIVATIONS AND METHODS OF FEMALE CYBERCRIMINALS IN INDIA

AUTHORED BY - ESHAN SINGHAL, ROHITASH & KAMAL HASME

ABSTRACT

This study paper explores the domain of cybercrime in India, with a particular emphasis on challenging gender preconceptions. It also examines the phenomenon of female cybercriminals in India. This study delves into the reasons and strategies utilized by female cybercriminals, thereby illuminating a frequently overlooked and undervalued faction within the realm of cybercrime.

This study aims to explore the underlying motivations that drive women to engage in cybercriminal activities, drawing upon a thorough literature review and empirical research. Additionally, the study examines case studies to provide insights into the significant involvement of females in digital-age crimes. Additionally, this study examines the hacking methodologies, strategies of social engineering, and digital platforms employed by female cyber offenders in India.

Furthermore, this study examines the ramifications of these findings inrelation to the mitigation of gender bias in cybercrime and proposes policy suggestions for effectively countering cyber threats in a manner that includes all genders. This research makes a valuable contribution to the greater academic conversation surrounding cybersecurity, gender equality, and crime prevention by challenging misconceptions and providing a more comprehensive understanding of female cybercriminals in India.

This article also examines the significance of gender-specific hurdles in societal, legal, and law enforcement domains in order to advance a just and impartial strategy for addressing cybercrime, irrespective of gender.

Keywords: Female Cybercriminals, Gender Stereotypes, Motivations,Cybercrime Methods

I. INTRODUCTION

The realm of cybercrime has historically been enveloped in enigma, fascination, and a narrative predominantly influenced by males. The representation of cybercriminals in popular media frequently portrays them as enigmatic individuals congregating in poorly illuminated spaces, concealing their identities behind hooded garments and computer displays. This portrayal has contributed to a prevailing prejudice that has predominantly marginalized a notable demographic: women. The issue of cybercrime continues to pose a significant concern in the contemporary digital era. However, there has been a notable lack of attention given to the reasons and techniques employed by female cybercriminals in India. This oversight can be attributed to a prevailing narrative that portrays them as uncommon outliers or passive participants in illegal activities.

The imperative to comprehend and investigate female cybercriminals in India has reached a heightened level of significance in the present context. The prevalence and sophistication of cybercrimes are increasing in tandem with the expansion of the digital realm. The proliferation of the internet and the escalating dependence on digital technology in India has engendered a host of novel prospects and complexities. The impact of cybersecurity concerns extends to both individuals and companies nationwide. However, it is important to acknowledge that gender dynamics significantly influence the experiences and motives of female cybercriminals.

The lack of adequate representation of women in the field of cybercrime research is a substantial limitation to our comprehension of the wider cyber- threat landscape. The issue of underrepresentation is not limited to gender equity alone, but also hinders the progress in devising effective measures to address cybercrimes. It is crucial to acknowledge that women are not exempt from participating in cybercriminal activities. Therefore, it is essential to comprehend their motives, strategies, and obstacles in order to promote a more inclusive and complete approach to cybersecurity.

The incidence of cybercrime in India has experienced a significant surge in recent times, presenting considerable risks to individuals, enterprises, and the country's cybersecurity framework (Potharaju, n.d.)[1]. Nevertheless, despite the increasing amount of scholarly work on cybercrime in India, there is a noticeable lack of research on the gender aspect of cybercriminal

[1] Potharaju, S. (n.d.). *Secure in India 2020*. KPMG. https://kpmg.com/in/en/home/insights/2020/12/secure-in-india-2020.html

behaviour.

The digital transformation in India has led to an increased dependence on technology and the internet. This shift has been accompanied by a rise in various forms of cybercrimes, including phishing, online fraud, data breaches, and cyber-bullying. KPMG India's report on "Cybercrime in India: Unlocking Hidden Risks" (2020) provides a comprehensive overview of the evolving cyber threat landscape in India, highlighting the need for a multifaceted approach to combat cybercrimes.

Gender disparities in cybercrime research have been evident worldwide. In India, this gap becomes more pronounced due to the underrepresentation of female cybercriminals in scholarly studies. Much of the existing literature on cybercrime in India tends to focus on male offenders (The Gender-Equal Cybercriminal Underground - Security News, 2023)[2]. This narrow focus has perpetuated the stereotype that women are less likely to engage in cybercriminal activities, an assumption that requires critical examination.

Stereotypes play a pivotal role in shaping perceptions and expectationsregarding the involvement of women in criminal activities, including cybercrime. Gender stereotypes have often painted women as passive victims rather than active perpetrators of cybercrimes (Holt, 2016)[3]. This skewed portrayal overlooks the complex motivations and methods employed by female cybercriminals and hamper the development of effective prevention and intervention strategies (Holt & Bossler, 2016)[4].

While limited in number, emerging studies are beginning to shed light onthe motivations and methods of female cybercriminals in various contexts. Research by Holt and Smirnova (2012)[5] suggests that women's involvement in cybercrime may be motivated by financial gain, personal vendettas, or ideological reasons, similar to their male counterparts. This research challenges the

---

[2] *The Gender-Equal Cybercriminal Underground - Security News*. (2023, February 28). The Gender-Equal Cybercriminal Underground - Security News. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/gender- in-cybercrime

[3] Chua, Y. T., & Holt, T. J. (2016). A cross-national examination of the techniques ofneutralization to account for hacking behaviors. *Victims & Offenders*, *11*(4), 534-555.

[4] Holt, T. J., & Bossler, A. M. (2015). Cybercrime in progress: Theory and prevention oftechnology-enabled offenses.

[5] Holt, Strumsky, & Smirnova. (2012, June). Examining the Social Networks of MalwareWriters and Hackers . *International Journal of Cyber Criminology*, *6*(1), 891–903. https://www.cybercrimejournal.com/pdf/holtetal2012janijcc.pdf

notion that female cybercriminals are driven solely by passive involvement or coerced participation.

II. RESEARCH QUESTION AND OBJECTIVES

This article seeks to explore the motivations and methods of female cybercriminals in India, shedding light on a demographic that has long remained in the shadows of cybercrime discourse. To achieve this, thefollowing research questions and objectives are as follows:

1. What motivates women in India to engage in cybercriminal activities?
2. What methods and techniques do female cybercriminals employ?
3. What challenges and obstacles do female cybercriminals encounter inIndia?
4. What are the legal and policy implications of female cybercriminalinvolvement in India?

III. MOTIVATIONS OF FEMALE CYBERCRIMINALS

It is imperative to acknowledge that motivations for engaging in cybercrime are multifaceted and can vary among individuals[6]. The incentives can be classified into three overarching categories, namely economic, personal, andpsychological ones.

1. Economic Motivations

Female cybercriminals in India, like their male counterparts, may be driven by economic factors such as financial gain. These motivations may include:

a) Financial Desperation: Certain individuals of the female gender may engage in cybercriminal activities as a result of financial hardships, lack of career prospects, or restricted access to economic avenues, perceiving such activities as a means to attain financial stability.

b) Profit and Financial Independence: Some women may view cybercrime as a profitable pursuit and may choose to participate in acts suchas phishing, identity theft, or fraud in order to attain economic autonomy.

2. Personal Motivations

Personal motivations can provide insight into the individual circumstances and personal goals that lead women to cybercriminal activities:

---

[6] K. M. (n.d.). Cybercrime Module 3 Key Issues: The Role of Cybercrime Law. CybercrimeModule 3 Key Issues: The Role of Cybercrime Law. https:////www.unodc.org

a) Revenge or Retribution: Certain female cybercriminals may engage in cybercrime as a strategy to retaliate or seek retribution against individuals, organizations, or institutions whom they perceive as having inflicted harm upon them.

b) Adventure and Thrill-Seeking: The allure of cybercrime may be particularly appealing to women who are drawn to the prospect of excitement and adventure. Engaging in hacking and criminal online activities can evoke a heightened sensation of excitement and a stimulating level of difficulty.

3. Psychological Motivations

Psychological factors play a significant role in understanding why women engage in cybercrime:

a) Anonymity and Disinhibition: The internet provides a certain level of anonymity, which facilitates the participation of individuals, including women, in cybercriminal activities without immediate repercussions.

b) Peer Influence and Social Networks: The involvement of women in cybercriminal acts can be attributed to several factors, such as peer pressure and influence exerted by their social networks[7]. This impact may stem from online communities that actively promote or legitimize such behaviour.

c) Psychological Disorders: In certain instances, the presence of underlying psychiatric problems or personality traits, such as narcissism or antisocial conduct, may potentially play a role in a female individual'sengagement in cybercriminal activities.

IV. CASE STUDIES

Some of the case studies of notable female cybercriminals in India are as follows:

Case Study 1: The "Dating" as tool to lure for extorting money

A software engineer residing in Bengaluru reportedly became a target of afraudulent scheme on a dating platform. As per the statement provided tothe law enforcement authorities by the victim Srinath, he becameacquainted with an individual named Rupali, who presented herself asArpitha, a teacher, using an internet platform designed for dating purposes. The woman initiated contact with him, leading to the commencement of a conversation on the messaging platform

[7] Little, W. (n.d.). Chapter 7. Deviance, Crime, and Social Control – Introduction toSociology – 2nd Canadian Edition. Chapter 7. Deviance, Crime, and Social Control –Introduction to Sociology – 2nd Canadian Edition. https://opentextbc.ca/introductiontosociology2ndedition/chapter/chapter-7-deviance-crime- and-social-control/

WhatsApp. She made a formalrequest to the victim, urging them to transfer a sum of ₹30,000 to a designated bank account. The rationale provided for this request was the hospitalization of her father in Kolkata. According to the complaint, she persistently urged him to send further funds, resulting in a cumulative amount of ₹59.72 lakh over a span of six months[8].

According to law enforcement officials, the Rupali with her husband allegedly devised a scheme to deceive individuals through online means. Rupali would access the website with the intention of ensnaring individuals of the male gender. The individual in question would opt to utilize photographs with professional models as their chosen profile picture.

Case Study 2: The "Nude Calls"

Cybercriminals have recently devised a novel approach to deceive, coerce, and illicitly obtain funds from individuals. With the rise in individuals'internet usage during the Covid-19, there has been a corresponding surge in the ingenuity of online fraudsters in their efforts to exploit unsuspecting victims. Cyber criminals have recently devised novel strategies, such as the Nude Video call[9] approach, to exploit individuals on popular social media platforms like WhatsApp and other video call-enabled platforms. Theseindividuals engage in fraudulent activities by initiating video calls to random phone numbers, during which a sexually explicit conversation takes place between a nude woman and the targeted individual. The perpetrators engage in the act of recording individuals conversing with the female party through the utilization of a screen recording application. Subsequently, they transmit the recorded video to the victims, accompanied by a demand for monetary compensation, under the threat of disseminating said video on various social media platforms.

Similarly a man loses an amount of 12.24 lakh approx.[10]. after receiving a friend request from a female on Facebook. There they shared whatsapp number to each other and female while doing a video call tempted him to remove clothes and thereby make a recording of it. She demanded money and in case of failure to give, she threatened him to post the video on several media

---

[8] *Woman dupes techie of ₹59 lakh*. (2018, June 26). The Hindu. https://www.thehindu.com/news/cities/bangalore/woman-dupes-techie-of-59- lakh/article24265285.ece

[9] *Madhya Pradesh: Now, online fraudsters using "Nude Video Call" trick to extort moneyfrom people | Bhopal News - Times of India*. (n.d.). The Times of India. https://timesofindia.indiatimes.com/city/bhopal/madhya-pradesh-now-online-fraudsters- using-nude-video-call-trick-to-extort-money-from-people/articleshow/77674964.cms

[10] *Man loses ₹12.24 lakh in Facebook sextortion scam*. (2022, June 11). Hindustan Times. https://www.hindustantimes.com/cities/mumbai-news/man-loses-12-24-lakh-in-facebook- sextortion-scam-101654969068149.html

platforms.

3: Case study: Cryptoqueen

In the initial days of June 2016, Dr. Ruja Ignatova, a 36-year-old female entrepreneur asserted that OneCoin was poised to emerge as the largest global cryptocurrency, facilitating universal payment capabilities. During her address, Dr. Ruja referred to OneCoin as the "Bitcoin Killer". She exclaimed that Bitcoin would no longer be a topic of discussion in two years.

Globally, individuals had begun allocating their resources towards OneCoin,with the aspiration of participating in this emerging revolution. The stolen documents obtained by the BBC reveal that individuals residing in theUnited Kingdom allocated a sum of about €30 million towards the acquisition of OneCoin during the initial half of 2016.

Ruja Ignatova assumed the moniker of "Cryptoqueen[11]." The individual in question made assertions to several individuals regarding the creation of a cryptocurrency intended to compete with Bitcoin, subsequently convincing them to allocate substantial financial resources amounting to billions. Subsequently, two years prior, her whereabouts were unknown. Jamie Bartlett conducted an extensive investigation over a period of several months for the Missing Cryptoqueen podcast, with the aim of unravelling the methods employed by the subject and determining her currentwhereabouts.

V. Case Study: Romance Scams

Romance scams involving female cybercriminals are not uncommon. These scams often involve building fake romantic relationships with victims and then requesting financial assistance. While not all romance scams in India involve female perpetrators, some have gained attention due to their use of social engineering tactics to deceive and defraud individuals. The research conducted by Norton[12] regarding the online behaviour of individuals in India revealed that online dating scams have resulted in significant financial losses. According to the survey respondents from India, the average amount lost owing to these scams was ₹7,966.

---

[11] Cryptoqueen: How this woman scammed the world, then vanished. (n.d.). BBC News. https://www.bbc.com/news/stories-50435014

[12] *Indians lost ₹7,966 on average in online dating scams: Report.* (2023, February 10). The Hindu. https://www.thehindu.com/sci-tech/technology/indians-lost-7966-average- involving-online-dating-scams-report-norton/article66492854.ece

These case studies provide insights into the motivations, methods, and legal consequences of female cybercriminals in India. They serve as examples of the diverse range of cybercrimes and the individuals involved in them,challenging stereotypes and shedding light on the complexities of this emerging field.

VI. Methods and Techniques Used by Female Cybercriminals

The methodologies and strategies utilized by female cyber offenders in India are diverse, encompassing a spectrum of approaches such as social engineering and intricate hacking endeavours. A comprehensive grasp of these tactics is important for law enforcement and cybersecurity experts in order to effectively tackle cybercrime.

Several prevalent forms of cybercrime include the following:

1. Hacking:

The act of hacking encompasses the illicit acquisition of entry into computersystems, networks, or databases. In India, female cybercriminals are known to utilize hacking tactics for a range of objectives, including but not limited to data theft, sabotage, and activism. One noteworthy instance is to the hacking collective known as "Legion," which consisted of a female participant and focused on high-profile individuals and organizations, thereby revealing confidential data in the year 2016[13].

2. Fraud:

Female cybercriminals frequently engage in fraudulent acts, encompassing money fraud and online frauds. Perpetrators may engage in the creation of fraudulent profiles on various social media platforms with the intention of deceiving unsuspecting individuals by assuming false identities. Anillustrative example is the well-known 'Sheena Bora murder case,' in which the perpetration of identity theft and deceitful communication played asubstantial role[14].

3. Identity Theft:

Identity theft is a pervasive form of cybercrime characterized by the unauthorized acquisition and

[13] Chesney, B., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107(6), 1753–1820. https://www.jstor.org/stable/26891938

[14] Sheena Bora murder case: Indrani Mukerjea talks about forensic discrepancies, “foulplay.” (2023, September 4). The Economic Times. https://economictimes.indiatimes.com/news/india/sheena-bora-murder-case-indrani- mukerjea-talks-about-forensic-discrepancies-foul-play/videoshow/103364783.cms

subsequent exploitation of personal information. Women who participate in cybercriminal activities may employ identity theft as a means to gain unauthorized access to financial assets or perpetrate other illicit activities. In the year 2022, law enforcement authorities in India apprehended a woman who employed a pilfered identity to engage in activities deemed antinational, thereby underscoring the pervasive prevalence of this form of criminal behaviour[15].

4. Social Engineering:

Female cybercriminals frequently employ social engineering strategies as a means of manipulating individuals into disclosing sensitive information.These individuals have the potential to assume the identities of reliable sources or employ tactics of emotional manipulation. Instances of female cybercriminals engaging in social engineering tactics encompass various forms such as romance scams and catfishing, hence resulting in detrimental consequences of both financial and emotional nature for the targeted individuals.

IV. LEGAL AND POLICY IMPLICATIONS

A. Exploring the Existing Legal Framework for AddressingCybercrime in India

India has made notable progress in the establishment of a comprehensive legal framework aimed at effectively tackling cybercrime. The Information Technology Act, 2000 serves as the principal legislation in India that regulates cybercrimes[16]. It has undergone multiple amendments in order to effectively address the continuously emerging cyber threats. The aforementioned legislation establishes a fundamental framework for the legal pursuit and prosecution of diverse forms of cybercrimes, encompassing activities like as hacking, identity theft, and online fraud.

Moreover, India has officially endorsed the Budapest Convention on Cybercrime, a treaty that promotes global collaboration in the detection and legal pursuit of cyber offenses[17]. The aforementioned global commitment highlights India's acknowledgement of the significance of addressing cyber threats on a worldwide level.

---

[15] *Chinese woman held for identity theft, anti-national activities, was living as monk in Delhi*. (2022, October 21). India Today. https://www.indiatoday.in/india/story/delhi-police- arrest-chinese-woman-for-involvement-in-identity-theft-anti-national-activities-2287948- 2022-10-21

[16] P. (n.d.). *A comparison of cybersecurity regulations: India*. PwC. https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a- comparison-of-cybersecurity-regulations/india.html

[17] *On global cybercrime, India votes in favour of Russia-led resolution*. (2019, November21). The Indian Express. https://indianexpress.com/article/india/on-global-cybercrime- india-votes-in-favour-of-russia-led-resolution-6130980/

B. Discussing Gender-Specific considerations within the Legal System

Although India's legislative framework for tackling cybercrime is extensive, it may not sufficiently encompass the gender-specific dimensions of cybercrimes perpetrated by women. In order to bridge this disparity, it is imperative for the legal system to take into account the subsequent gender- specific factors:

a. **Gender-Sensitive Legal Responses:** It is imperative for the legal system to incorporate gender-sensitive methodologies in the investigation and prosecution of cybercrimes perpetrated by women. This entails comprehending the distinct incentives employed by female cybercriminals and adapting solutions accordingly.

b. **Rehabilitation and Support:** The legal system should broaden its approach beyond punitive measures and incorporate rehabilitation and support services to effectively address the root causes that contribute to the engagement of female cybercriminals in illicit activities. This mayencompass many interventions such as counselling services, educational initiatives, and programs aimed at fostering skill development.

c. **Privacy and Victim Protection:** In the context of the legal system, it is imperative to accord utmost importance to safeguarding the privacy and ensuring the safety of victims, with a particular emphasis on instancesinvolving cyber-bullying, harassment, and the dissemination of revenge porn. It is imperative to implement specific measures aimed at protectingthe rights and ensuring the well-being of victims.

d. **Training and Sensitization:** It is imperative that legal professionals, encompassing judges, lawyers, and law enforcement personnel, undergocomprehensive training and sensitization pertaining to gender-related matters within the realm of cybercrime. This measure has the potential to mitigate biases and promote equitable treatment of female cybercriminals.

C. Suggesting potential Policy Changes or Improvements

In order to effectively tackle the gender-specific dimensions of cybercrime perpetrated by women, it is imperative for policymakers in India to deliberate about and implement the following policy modifications and enhancements:

a. **Gender-Responsive Legislation:** It is recommended that policymakers undertake a comprehensive evaluation of current cybercrime legislation and deliberate on potential revisions or novel measures that explicitly target gender-related cybercrimes, while also taking into account the unique requirements of female offenders and victims.

b. **Support for Gender-Equal Access to Technology:** It is imperative that policies be

formulated to actively encourage and facilitate gender parity in terms of access to technology, education, and employment prospects within the domains of cybersecurity and digital technology. This measure has the potential to address the gender disparity in cybercriminal activities.

c. **Victim Support Services:** It is recommended that policymakers dedicate resources towards the establishment of victim support programs that specifically address the needs of those impacted by cybercrimes that are gender-specific in nature. The aforementioned services encompass helplines, counselling services, and legal aid.

d. **Gender-Responsive Training:** This proposal aims to design and implement training programs and activities that will enhance the awareness and understanding of gender-related concerns in the realm of cybercrime among law enforcement personnel, legal professionals, and members of the court. Ensuring equitable and suitable handling of instances involving female cybercriminals will be guaranteed.

e. **Research and Data Collection:** Promote the investigation of gender-specific cybercrimes in order to enhance comprehension of their extent and consequences. Efforts pertaining to data collecting should prioritize the acquisition of gender-disaggregated information pertaining to cybercrime. Therefore, it is imperative to acknowledge and account for gender-specificfactors within the legal system and policy framework in order tosuccessfully combat cybercrime and guarantee that solutions are just andimpartial for all individuals, irrespective of their gender. By acknowledging the distinct obstacles and motives that female cybercriminals face, India candesign more focused and efficient strategies to address this ever-changingmenace.

V. GENDER STEREOTYPES AND CYBERCRIME

A. Investigating the Influence of Gender Stereotypes on Female Cybercrime Involvement

The examination of the correlation between gender stereotypes and participation in cybercrime is a complex and captivating field of research. Gender stereotypes refer to predetermined beliefs and societal expectations on the prescribed roles, behaviours, and capabilities of individuals, which are influenced by their gender. The impact of stereotypes on female participation in the digital world of cybercrime can be both reinforcing and inhibiting.

1. **Perpetuation of Stereotypes:** An important factor to contemplate is the potential role of gender stereotypes in perpetuating the underrepresentation of women in the realm of cybercrime. Throughout history, cybercriminal actions have largely been linked to male perpetrators. These prejudices frequently depict women as being less proficient in technical matters or as individuals who are less inclined to participate in unlawful onlinebehaviours. Consequently, the involvement of women in cybercrime may be facilitated due to reduced suspicion and scrutiny, allowing them to operate covertly.
2. **Challenging Stereotypes:** On the other hand, it is worth noting that gender stereotypes can present a counterbalancing force by posingchallenges to the participation of females in cybercrime activities. Certain individuals of the female gender may strategically leverage prevailing preconceptions to their benefit, capitalizing on the widely held belief that they are less inclined to engage in cybercriminal activities. Female cybercriminals may potentially execute their crimes with reduced scrutinyby adopting a less intimidating or suspicious demeanour. This phenomenon prompts inquiries on the potential underestimation of female cybercriminals and, as a result, the potential subversion of gender stereotypes within this particular domain.

B. <u>The Role of Media and Public Perception in Shaping Gender Stereotypes and Cybercrime</u>

The influence of media and public perception is significant in developing and perpetuating gender stereotypes, particularly in relation to the involvement of individuals in cybercrime. These factors have the potentialto either perpetuate conventional prejudices or facilitate their evolution.

1. **Media Portrayal**: The media frequently assumes a prominent role in the perpetuation of gender stereotypes. The depiction of cybercriminals in popular culture and news media has the potential to perpetuate the perception that hackers are mostly male. This depiction has the potential to deter and dissuade female engagement in cybercriminal activities. Conversely, the media has the potential to contest these prejudices by showcasing female cybercriminals who violate traditional gender standards, thereby illuminating the wide range of profiles within the realm of cybercriminal activity.
2. **Public Perception:** The importance of media coverage and cultural views on public perception of gender stereotypes and cybercrime has been widely acknowledged. The capacity of individuals to spot and report cybercrimes involving women can be influenced by their impressions of the stereotypicalappearance of a cybercriminal. Public awareness

campaigns and educationalinitiatives have the potential to play a significant role in altering prevailing beliefs and questioning gender norms. Furthermore, the manner in which law enforcement agencies and judicial systems address female cybercriminals can be subject to the influence of public opinions, whichmay result in discrepancies in sentencing and treatment based on gender.

Overall, the correlation between gender stereotypes and cybercrime is a multifaceted phenomenon. The perpetuation and challenge of female engagement in cybercrime can be influenced by gender stereotypes, which are subject to individual perception and utilization. The influence of media and public perception is significant in the construction of stereotypes, as it can either strengthen established standards or facilitate their evolution. Consequently, these factors have a profound effect on the interplay between gender and cybercrime within society. Additional research is required in order to gain a more comprehensive understanding of these processes and formulate effective measures to mitigate gender prejudice within the domain of cybercrime.

VI. CONCLUSION

The presence of female cybercriminals in India presents a significant departure from conventional preconceptions and underscores the importance of adopting a nuanced and gender-sensitive approach in combating cybercrime. Gaining insight into the motivations, methodologies, difficulties, and barriers encountered by female cybercriminals is crucial in order to formulate efficacious legal and legislative measures.

The legislative structure in India pertaining to cybercrime, which is primarily established by the Information Technology Act, has established a robust basis for effectively dealing with digital security risks. Nevertheless, it is imperative for it to undergo adaptation in order to incorporate gender- specific factors. The recommended measures encompass the implementation of legal solutions that are sensitive to gender, the prioritization of rehabilitation and support services, the protection of the privacy and rightsof victims, and the provision of training and sensitization programs for legal professionals.

Policymakers assume a pivotal role in directing the response to cybercrimes that specifically target individuals based on their gender. Various strategies can be used to address gender disparities, including the implementation of legislation that is responsive to gender issues, the promotion of

equitable access to technology for all genders, the establishment of support services for victims, the provision of training programs tailored to specific genders, and the encouragement of research and data gathering in this area.

By acknowledging and mitigating the gender-specific dimensions of cybercrime, India has the potential to cultivate a more egalitarian, fair, and efficient strategy for combating cyber threats. The process of challenging stereotypes encompasses not only recognizing the many characteristics of individuals engaged in cybercriminal activities, but also adopting proactive measures to hinder, intervene in, and rehabilitate these perpetrators. In essence, with a comprehensive examination of the distinct encounters of female cybercriminals, India can progress towards a digital environment that is both secure and inclusive for its entire populace.