IJAPS, Vol. 19, No. 1, 23–49, 2023

A SOCIOLOGICAL STUDY OF CYBERCRIMES AGAINST WOMEN IN INDIA: DECIPHERING THE CAUSES AND EVALUATING THE IMPACT ON THE VICTIMS

*Subhra Rajat Balabantaray**
Department of Economics and International Business, School of Business,
University of Petroleum and Energy Studies, Kandoli Campus, Dehradun,
Uttarakhand-248008, India
E-mail: subhrarajat@gmail.com

*Mausumi Mishra***
Centre for the Study of Social Systems, Jawaharlal Nehru University,
New Mehrauli Road, JNU Ring Rd, New Delhi, 110067, India
E-mail: mausumimishra87@gmail.com

*Upananda Pani****
Department of Economics and International Business, School of Business,
University of Petroleum and Energy Studies, Kandoli Campus, Dehradun,
Uttarakhand-248008, India
E-mail: upananda.pani@gmail.com

Published online: 15 January 2023

To cite this article: Balabantaray, S. R., Mishra, M. and Pani, U. 2023. A sociological study of cybercrimes against women in India: Deciphering the causes and evaluating the impact on the victims. *International Journal of Asia Pacific Studies* 19 (1): 23–49. https://doi.org/10.21315/ijaps2023.19.1.2

To link to this article: https://doi.org/10.21315/ijaps2023.19.1.2

ABSTRACT

The growing use of the internet has provided a conducive platform for miscreants to engage in the misuse of information and communication technology (ICT). It has resulted in a potential threat to individuals in terms of cybercrimes. In general, cybercrimes are increasing at a rapid pace in India. The most vulnerable group targeted in cybercrimes in India has been women and girls. Using purposive sampling method for the selection of sample, this study focuses on cybercrimes against women in India and their impact on the victims. Awareness about cybercrimes is minimal. Historically, women have been subjected to various kinds and forms of discrimination and crimes, the newest being cybercrimes.

Results exhibit that computer literacy is higher among males than females, which is a factor in women being more vulnerable to cybercrimes. The suppression of cybercrimes affects the victim psychologically through depression, fear, anxiety, and withdrawal from cyberspace. To overcome these kinds of effects, victims often share the situation they have faced with friends, close acquaintances, and family members.

Keywords: Cybercrimes, violence, women, India, internet

INTRODUCTION

Women in India experience violence in different corners of the country. Violence can happen in various places such as homes, public places, or offices (Chakraborty et al. 2021). Saravanan (2000) states that violent crimes against women could be partially attributed to the false assumption of male superiority. In many societies, most gender-based violence is considered normal. Various social and cultural factors are responsible for the emergence and dissemination of violence against women. Past research also exhibits the fact that a substantial percentage of women, irrespective of the social or economic background they come from, believe that men have the autonomy to discipline them, especially when they fail to cook food on time or behave in a manner as desired by their husbands (Visaria 2008; Sikweyiya et al. 2020). Moreover, abused women usually justify their husbands' behaviour to rationalise the violence they experience (Ökten 2017; Hadi 2017; Ravindran and Shah 2020; Mondal and Paul 2021).

The irony is that individuals in Indian society tend to worship women as Goddesses, but there is still a surge in cases of violence against women. Historically, women in India were vulnerable to sexual harassment, domestic violence, street violence, rape and rape threats, acid attacks, molestation, trafficking, female infanticide, and honour killing. In recent years, 31% of married women experienced domestic violence committed by their partner in 2015 and 2016 (Mondal and Paul 2021). Ravindran and Shah (2020) reported a 131% increase in domestic violence cases in May 2020 in India.

Gupta (2014) states that the number of reported cases against women in India is significantly less than the actual number of cases. Less than 1% of incidents of sexual violence by husbands were reported to the police. Similarly, only about 1% of incidents of physical violence by other men, and 2% of incidents of physical violence by husbands were reported. Singh (2015) highlights that despite various feminist movements striving toward women's empowerment, violence against women is far from over. The government of India has various legislations to address the violence against women; however, crimes against women are on the rise (Chakraborty et al. 2021). Cyber violence is a new kind of violence targeted against women. In modern-day India, women are experiencing a higher degree of cybercrimes due to the increasing encroachment of technology into our lives and the increase of time spent on the cyberspace.

BACKGROUND

Technology has become such an essential and integral part of everyday life for human beings and cannot be ignored. Imagining a life without a smartphone, tablet, laptop, or desktop is a daunting task. The excessive demand has created a huge market for these gadgets. During the 1990s, internet usage was minimal not only in India, but also around the world. However, since the 1990s, the rate and degree of internet users have grown exponentially. Table 1 shows the trend of internet users since the 1990s. It exhibits the gradual surge of individuals using the internet since the start of the 21st century.

Table 1: Internet connectivity from 1990–2017

Country	Number of internet users			
	1990	2000	2010	2017
India	–	5.56 million	92.32 million	391.26 million
United States of America	1.98 million	121.48 million	221.27 million	245.43 million
Canada	99,970	15.77 million	27.44 million	33.08 million
Russia	–	2.89 million	61.56 million	109.44 million
China	–	22.79 million	466.40 million	765.37 million

Source: Our World in Data (OWID) based on World Bank and UN world population prospects, 2017 (Alamo et al. 2020).

In the contemporary world, the usage of the internet is prominent for every person and has become an indispensable part of human life (Kandpal and Singh 2013; Singh et al. 2014; Chudasama et al. 2020; Mansi and Agarwal 2020; Yadav et al. 2021; Chudasama and Solanki 2021; Viraja and Purandare 2021). There has been significant growth in internet usage (Ch et al. 2020; Viraja and Purandare 2021). The internet has become an essential commodity (for each individual in every household) in the move towards digitalisation

(Castiglione et al. 2018; Srivastava and Yadav 2014). Modern-day individuals perform various duties and tasks with the help of the internet, ranging from office responsibilities to household chores (Sawaneh 2020; Zahoor and Razi 2020; Pajankar 2020). Online shopping is one such phenomenon, which has "eased the exertion on human lives" (Yasin et al. 2021). Starting from easy access to information to quick and fast communication among peers and others through social networking sites are some of the usages of the internet. Moreover, it has enhanced efficiency, resulting in cost-effectiveness and expedited productivity at the individual, household, and societal levels (Singh 2018).

In the 2000s, internet could be accessed only on desktops and computers, which were restricted to urban centres. However, the scenario has changed drastically over the past one and half decades. With the advent of smartphones, the internet is very conveniently available, thanks to cheap data plans. Kaur (2015) has stated that these reasons have contributed significantly to the growth of internet users. With the voluminous growth in the accessibility of individuals to the internet, more people are likely to be vulnerable to various cybercrimes (Khudhair 2021).

The growing use of the internet has provided a conducive platform for miscreants to engage in the misuse of information and communication technology (ICT) and this issue has resulted in a potential threat to individuals in terms of cybercrimes. In general, cybercrimes are increasing rapidly in India (Joshi and Singh 2013; Kethineni 2020). Studies have corroborated the fact that the increased level of internet use enhances the level of vulnerability as well (Ch et al. 2020; Mehta and Singh 2013; Tiwari et al. 2016; Meena et al. 2020; Iqbal and Beigh 2017; Sarmah et al. 2017; Chatterjee et al. 2019). The modern-day world, especially India, has experienced a tremendous increase in cybercrimes (Malar 2012; Dalla and Geeta 2013; Kethineni 2020; Deora and Chudasama 2021; Elavarasi 2021; Khudhair 2021; Barik et al. 2022). However, it is estimated that only 10% of cybercrimes are reported, and of the ones reported, only 2% get registered (Kshetri 2016; Meena et al. 2020). In cyberspace, women and children are the most vulnerable group facing the grave consequences of cybercrimes (Halder and Jaishankar 2011; Agarwal and Kaushik 2014; Singh 2018; Dogra and Kalra 2018; Chaudhary 2019; Datta et al. 2020; Poulpunitha et al. 2020; Panwar and Sihag 2020; Banerjee and Singh 2021). Globally and especially in India, cybercrimes against women have increased significantly (Saha and Srivastava 2014; Singh 2015; Halder and Jaishankar 2016; Ahmed et al. 2017; Chaudhary 2019; Kaphle 2019; Banerjee and Singh 2021). Sarkar and Rajan (2021) have highlighted that cyber violence extends various degrees of sexual violence experienced by women and often has manifold impacts. This study aims to find the reasons behind the increase in cybercrimes against women in India and their effects on the victims.

STATEMENT OF THE PROBLEM

The usage of the internet comes with a cost and has a certain degree of disadvantages and negative connotations as well (Goyal 2012; Kaur 2015; Ahmed et al. 2017; Anisha 2017; Singh 2018; Dogra and Kalra 2018; Mansi and Agarwal 2020; Sawaneh 2020; Pajankar 2020); for instance, hacking is a major drawback. The internet cannot be blamed as it is neutral (Joshi and Singh 2013) and does not contribute to cybercrimes on its own; however, it provides scope and opportunity for potential cybercriminals to further their criminal agenda by using extremely updated and sophisticated tools (Kundi et al. 2014). Hence, it has created a sense of fear and insecurity among various users. Several scholarly studies have established that social networking sites are "used to find the identity of interested people" (Dalla and Geeta 2013: 997); they are also misused to spread fake news and instigate communal violence in the country. Pornography has become a worldwide business that has significantly increased crimes against women and created fear among female internet users. With the global reach of the internet, cybercrime has emerged as a new form of crime (Rao et al. 2016; Mansi and Agarwal 2020). It includes a spectrum of activities, and the most prominent ones are bot-networks, cross-site scripting, cyberbullying, cyber flirting, cyber hacking, cyber morphing, cyberstalking, cybersquatting, email spoofing, hacking, revenge porn, and phishing (Goyal 2012; Kaur 2015; Tiwari et al. 2016; Halder 2017a, b, 2015; Wadhwa and Arora 2017; Singh 2018; Wavare 2018; Chudasama et al. 2020; Datta et al. 2020; Panwar and Sihag 2020; Zahoor and Razi 2020; Deora and Chudasama 2021).

The reduction of gender inequality as well as women's empowerment are important objectives of the United Nations Sustainable Development Goals adopted in 2015 (Pogge and Sengupta 2015). Moreover, the Constitution of India ensures various rights, including the freedom of speech and expression, safeguarding individuals' privacy, and ensuring that citizens live dignified lives. However, women are repeatedly looked down upon, humiliated and treated like "second-grade citizens" (Halder and Jaishankar 2016). Moreover, with the increase in cybercrimes, especially against women, the constitutional promise of equality for all is threatened repeatedly. The rapid growth of ICT and the availability of low-cost internet services have increased the popularity of the internet (Srivastava and Yadav 2014). The current pandemic caused a dramatic shift as internet consumption rose by 13% in India since the lockdown (Jain et al. 2020). There was a significant rise in data usage worldwide amidst the COVID-19 pandemic and the global lockdowns, which began in March and April 2020 (Dhapola 2020). The rise of internet usage has increased criminal activities in the virtual world and created insecurities in women's lives (Singh 2015; Chaudhary 2019; Pawar and Sakure 2019; Mansi and Agarwal 2020; Sawaneh 2020).

The pandemic has forced digitisation in many sectors, especially education and financial transactions. Women and girls using the internet for the first time have a limited understanding of privacy policies and hence, are susceptible to cybercrimes (Mansi and Agarwal 2020). The increasing rate of cybercrimes against women has made them insecure about using the internet, thereby broadening the picture of gender inequality. Hence, it is imperative to understand the causes behind the increasing cybercrimes against women and evaluate their impact on the victims, especially women.

REVIEW OF LITERATURE

Scholarly studies have tried identifying the major victims of cyberstalking and their level of awareness concerning the cybercrimes. They have also identified various types of stalkers, the motivation behind such crimes, and their personalities. The studies have revealed that there is a lack of minimal awareness among individuals and that they are becoming easy prey to the criminals (Datta et al. 2020; Nappinai 2010; Srivastava and Yadav 2014).

Hassan et al. (2020) have documented the extent of cyber violence targeted against females (above 18 years of age). The study has tried to understand various aspects, such as how the respondent is exposed and its impact on exposed females, i.e., psychologically, socially, and physically and documented their response mechanism. In a similar study, Singh (2018) has equated the various types of violence committed against women as similar to that of the violation of human rights, which is a justified argument. The author has further pointed out that various types and degrees of violence have been targeted against women, and there is no end to the vulnerability of women in the paper that evaluates the impact of cyber violence against women in India. Halder and Jaishankar (2016) have analysed the modern-day cybercrimes targeted against women. The authors have revealed the reasons for the enhanced rate of cybercrimes against women in India. Moreover, they believe that the absence of a uniform law to address the concerns in cyberspace is worsening the situation.

Saxena et al. (2012) have discussed the necessity of cyber security and the issues and challenges faced at organisational and personal levels. They have focused on various mechanisms to initiate large-scale awareness at the foundation level, for which they have advocated for changes in the education system. They have highlighted that the teachers are ignorant of cybersecurity threats and that no training or education regarding information security is provided to the students. Moreover, it is not practical even if provided, and students tend to forget that easily if it is not taught practically. They have also recommended improvements to be made at the classroom level to make students aware of cybercrime, hacking, and cyber theft.

Sankhwar and Chaturvedi (2018) have highlighted the number of cybercrime cases registered in 2016. The authors explain the different and most common types of cybercrimes and different sections of the Information and Technology Act 2000. They have briefly mentioned the major problems with formulation, implementation of policies, data collection, and the problems victims face in reporting the incident. They have provided some suggestive measures and a solution model of three pillars, i.e., education, empowerment, and legal recourse to deal with cybercrimes.

Shan-A-Khuda and Schreuders (2019) have studied the local area variation in cybercrime victimisation. The data for the study were collected from the recorded cybercrime incidents by the police in England. The study's results try to provide an insight into cybercrime victimisation and its relation to demographics and area variation.

Barker and Jurasz (2019) have emphasised the issue of violence and harassment against women. They have examined the importance of social media platforms for women to express their opinions on public and political issues and how these rights are severely affected by the increase in online violence committed against women. Their paper has considered the implications of online misogyny and online violence against women. Yar and Drew (2019) have analysed gender-based victimisation, toxic masculinity, and online misogyny. They have discussed the progress made by introducing updated laws in countries such as Australia, Wales, and England to criminalise online abuse. They concluded the findings to suggest some of the best practices to prevent online abuse.

Luong et al. (2019) have discussed the initiatives undertaken by the Vietnam government to address the concern of cybercrimes. The paper has analysed this using literature, official data available, reports, and legislative frameworks. The authors argue the ineffectiveness of the government and law enforcement agencies in combating cybercrimes. The paper has identified the challenges in Vietnam, such as the unskilled workforce and technology to deal with crimes in cyberspace. They have recommended further research by the various stakeholders, including planners, policymakers, and personnel related to law enforcement.

CONCEPTUALISING CYBERCRIMES

Cybercrimes are considered an illegal and criminal activity against an individual or a group by the employment of digital technology and networks, including the usage of the internet via devices such as computers, phones, tablets, and other technologies to inflict mental harm directly or indirectly to the victim (Anisha 2017; Backe et al. 2018; Chaudhary 2019; Kandpal and Singh 2013; Kashyap and Chand 2020; Malar 2012; Singh et al. 2014; Sharma and Alam 2016; Wadhwa and Arora 2017; Wavare 2018; Varalakshmi 2020; Zahoor and Razi 2020). Cybercrimes can also refer to "illegal trespass into the computer system or database of others, manipulation or theft of stored or online data, or sabotage of equipment and data" (Ompal et al. 2017: 5). The most prominent types of cybercrimes are: against individuals, against society, and against government or organisations (Singh et al. 2014; Tiwari et al. 2016; Singh 2018; Zahoor and Razi 2020).

The cybercrimes against an organisation include the data theft of confidential information, denial of service (DoS) attack to disrupt the services, email bombing, Trojan horse malware to gain access to users' systems, and salami attack to access bank account and credit card details. Cybercrimes against society include forgery, making false documents, signatures, and web jacking. The hacker creates a fake web page and asks for sensitive data such as passwords.

The cybercrimes against women include posting hurtful words, derogatory comments, cyberstalking, harassing with insulting messages, and posting fake information. Such acts can have a catastrophic impact on many, especially young adults. Women active on social media receive more threats or comments that attack their safety and freedom of expression in "male-dominated spaces" (Sobieraj 2018). Cybercrimes/cyber violence on social media can create various impacts (social, economic, and psychological) on female victims. The atmosphere of male dominance created via cybercrimes can cause shame and fear in the minds of women and girls (Sarkar and Rajan 2021: 4). Social media has empowered women (Halder and Jaishankar 2009) and provided them a platform to express their thoughts, stand in unity, and to protest and fight for equality, justice, and freedom with like-minded people. On one hand, social media is the backbone of women's empowerment; on the other hand, social media has made women's lives more vulnerable.

CYBERCRIMES IN INDIA: AN ASSESSMENT

There has been an increasing trend of cybercrimes in India (Datta et al. 2020; Kethineni 2020). Technically skilled cybercriminals are engaged with new crime trends by employing new technology. It is needless to point out that cybercrimes play a devastating role in India, causing a tremendous loss to the government and society. The more pressing issue is that criminals can often conceal their identities (Joshi and Singh 2013) successfully. Table 2 presents the number of reported crimes in India from 2010 to 2019. However, this does not provide a true picture of the actual number of crimes committed as a huge number of cases remain unreported.

Table 2: Total number of reported cybercrimes in India (2010–2020)

Year	Number of reported cybercrimes in India
2010	1,322
2011	2,213
2012	3,477
2013	5,693
2014	9,622
2015	11,592
2016	12,317
2017	21,796
2018	27,248
2019	44,735
2020	50,035

Source: National Crime Records Bureau (NCRB 2022).

Evaluation of Cybercrimes against Women in India

Since the internet has become an important necessity for each individual, more time spent online results in potential targets for the miscreants. Various online services such as banking, file sharing, and shopping on e-commerce sites make individuals vulnerable to fraud or phishing attacks. The majority of the cybercrimes reported from India are phishing, pornography, cyberstalking, and cybersquatting. It was also found out that most of the theft related to information is usually done by employees currently working in the organisation or those who have left the organisation. Hackers commit approximately one-third of the information theft. The cybercrimes targeted against women are massively under-reported, as women in India are mostly unaware of such criminal offences (Jain 2017; Chaudhary 2019). Women are blamed for outcomes over which they have no control. Even though women often are victims of cybercrimes, they prefer to maintain silence as honour is attached to female members of the family (Kaphle 2019; Chaudhary 2019).

The innovations and technological advancements in India are the outcomes of the initiatives such as Digital India, Bharat Net, and E-hospital to empower the citizens digitally. Digitalisation has enhanced various sectors in India, such as the economy, education and governance, but it has also increased cybercrimes exponentially every year (Sankhwar and Chaturvedi, 2018). Women voicing their opinion and taking a stand for their rights on the internet are ultimately cyberbullied or trolled, and threatened.

OBJECTIVES AND RESEARCH QUESTIONS

The aims and objectives of the current research are:

1. To analyse the causes of increasing cybercrimes against women in India.
2. To examine the impact of cybercrimes on the female victims.

Here are the following research questions:

1. What are the prime and subsidiary causes of cybercrimes?
2. What are the effects of cybercrimes on the victims?
3. What are the social consequences of cybercrimes on women and girls?
4. What are the coping mechanisms and strategies developed by the victims?

RESEARCH METHODOLOGY

Sampling Procedure

A purposive sampling method for the selection of samples was employed. The study focused on cybercrimes against women in India and their impact on the victims. The literature review has established that women are the most vulnerable group and soft targets of cybercriminals. Hence, this study focused on women as respondents and the questionnaire was only sent out to women and girls.

The current study was carried out with the help of Google docs. Email, WhatsApp, and Facebook were used to send out the questionnaires to various respondents located across India. The survey questionnaire was sent to the respondents, and a statement highlighted the study's purpose to enable a higher degree of participation and response. The study spanned from 1 January 2021 to 30 April 2021.

During this period, 396 responses were received. However, only 341 responses were complete. Moreover, several inconsistencies were found, and some of the responses were missing from the respondents. Hence, these 341 responses, which were complete, were considered for the study. Thus, the sample size for the research was 341.

Recruitment of Participants

Since the study evaluates cybercrimes against women, it is imperative to understand the same from their perspective. Hence, it was decided that all the respondents should be female. Past studies have identified that women from the 16–35 age group are the most vulnerable to cybercrimes (Datta et al. 2020). Hence, this age group was selected for the study.

Data Collection Tool

A pre-tested questionnaire in the English language was designed. The questionnaire was divided into three sections as follows:

Section I: General profile and basic information of the respondents.

Section II: This section contained questions relating to the causes of cybercrimes.

Section III: This section contained the issues and statements regarding cybercrimes and their impact on the victims and their mechanisms to deal with cybercrimes.

The questionnaire content was thoroughly examined to ensure the eradication of ambiguous questions. The pilot data collection was done on eight females to evaluate the clarity and comprehension of questions and assess the amount of time required to complete the questionnaire.

Ethical Considerations

Confidentiality was maintained during and after the collection of information from the respondents. The questionnaire contained a section right at the start, which offered ample explanation regarding the study's purpose, aims, objectives, and informed consent. A request was made regarding the informed consent of the respondents who were informed that the study was about evaluating cybercrimes against women in India. Adequate information regarding respondent anonymity and voluntary participation in the study was provided to the respondents.

As is the case with online surveys, the authenticity of the information provided by the respondents cannot be vouched. However, we have to believe in the integrity of the respondents and assume that they have given accurate responses.

RESULTS

The results revealed that all the respondents were female, and it was purposive considering the study aimed to understand cybercrimes from the women's perspectives (Table 3). The first age group (16 to 25 years old) formed 57.8% of the respondents while the second age group (26 to 35 years old) formed 42.2% of the respondents. As pointed out earlier, the average time spent on mobile and internet usage had increased, and the results corresponded to this fact as 39.8% of the respondents spent 1–3 hours and 28.7% spent 4–6 hours on the internet. The results also revealed that 81.6% of the respondents update their personal information on social media, which allowed cybercriminals to misuse such information. It was pertinent to examine the level of understanding of the respondents regarding the awareness of cybercrimes, cybersecurity and cyber laws. In this study, 57.8% of the respondents showed absolutely no knowledge about cybercrimes, cybersecurity and cyber laws. Hence, this made it easier for cybercriminals to find their targets.

Table 3: General profile and basic information

Question	Response	Number	Percentage
Gender	Female	341	100.0
Age	16–25	197	57.8
	26–35	144	42.2
Mobile and internet usage	Less than 1 hour	52	15.2
	1–3 hours	136	39.8
	4–6 hours	98	28.7
	More than 6 hours	55	16.3
Do you update your personal information on social media?	Yes	278	81.6
	No	63	18.4
Awareness of cybercrimes, cybersecurity and cyber laws	Completely aware	53	15.5
	Slightly aware	91	26.7
	Not aware	197	57.8

Table 4 exhibits information relating to victims' exposure to various cybercrimes. First, 68.3% of the respondents had faced some kind of cybercrime during the past year. Moreover, 36.9% revealed that they had experienced cyber violence more than twice last year. Hence, it can be inferred that victims are also regularly being targeted. A question was posed to the respondents as to whether they knew the perpetrator, and only 18% of the respondents opined that the offender was a known individual. In the majority of the cases, the victim did not know the perpetrator of the crime, and various scholarly studies substantiated the same finding. It was also found that in most cases (82%), the offender was not known to the victim. Some of the previous studies also established the same fact. It was found that social media happened to be the mode where the degree of vulnerability was quite high. In this study, 69.9% of the respondents opined that their exposure mode was social media.

Table 4: Exposure to cybercrimes

Question	Response	Number	Percentage
Exposure to cybercrimes (year 2020)	Yes	233	68.30
	No	108	31.70
Number of times exposed to cybercrimes (year 2020)*	Once	96	41.20
	Twice	51	21.90
	More than twice	86	36.90
Do you know the offender?*	Yes	42	18.00
	No	191	82.00
Mode of exposure*#	Email	28	12.40
	Mobile phone	96	41.20
	Social media	161	69.90
	Others	11	4.70
Types of cybercrimes faced by victims*#	Cyberstalking	165	70.82
	Harassment via email	128	54.94
	Cyber defamation	23	9.87
	Morphing	14	6.01
	Email spoofing	26	11.16
	Hacking	12	5.15
	Cyber flirting	67	28.76

Notes: *As per the study's findings, 233 out of the 341 respondents were exposed to cybercrimes; hence, the responses to this question were from the same number of respondents.
# Respondents gave multiple responses

Table 5 depicts the findings relating to the causes of cybercrimes and their impact on victims. Participants believe that ignorance about cyber laws and increased use of mobile are the two primary reasons for increased cybercrimes. On the issue of silence over the cybercrimes faced, 52.7% of the respondents opined that they kept quiet, anticipating a certain degree of victim-blaming. Moreover, 35.6% stated that they were not aware of cybersecurity laws. There was a mixed bag of responses regarding the action they had initiated from their end to respond to the cybercrimes committed against them. For example, 32.6% said they had blocked the perpetrators of the crime, followed by 19.3% who ignored such activities. However, 9.4% of respondents claimed to have stopped using social media after the incident they faced. Another problematic issue was the minimal level of awareness about the Indian Penal Code (IPC) to punish the offenders. A majority of the respondents (75.5%) stated that they do not have any such awareness to punish the culprits. Only a meagre percentage of respondents (11.5%) stated that they have a considerable idea of such legislation to punish the culprits. An examination of the impact on the victim revealed some very shocking results; 69.9% of the victims faced psychological issues due to cybercrimes. The impact was also felt socially, as 20.6% of respondents opined that cybercrimes had a certain degree of impact on their social lives.

Table 5: Reasons for cybercrimes and impact on victims

Question	Response	Number	Percentage
Reasons for increase in cybercrimes#	Lack of computer literacy	44	18.8
	Ignorance of cyber laws	83	35.6
	Increased mobile and internet use	76	32.6
	Unemployment of educated youth	43	18.4
	Lower conviction rate for cybercrimes	37	15.9
Reasons for silence of cybercrime victims*	Not aware of cybersecurity laws	83	35.6
	Fear of victim-blaming	123	52.7
	Fear of isolation	11	4.7
	Non-accessibility to cyber police stations	16	6.8
Action taken in case of harassment*	Block	76	32.6
	Report	37	15.9
	Ignore	45	19.3
	Warning and blocked	53	22.8
	Stopped using social media	22	9.4
Awareness about IPC to punish the offenders*	Yes	27	11.5
	No	147	63.9
	Slightly aware	59	25.3
Mechanisms to protect identity on social networking sites#	Give minimum information	176	75.5
	Change security settings to enhance privacy	53	22.7
	Adjust information depending on trust level	36	15.4
	Use dummy email accounts	17	7.2
Impact of cybercrimes on victims*#	Psychological	163	69.9
	Social	48	20.6
	Economical	8	3.4
	No effect	41	17.5

Notes: *As per the study's findings, 233 respondents were exposed to cybercrimes; hence, the responses to this question were from the same number of respondents.

#Respondents gave multiple responses

DISCUSSION

The results above have revealed that the increased usage of mobile and the internet has made women and girls more vulnerable to cybercriminals. Several scholarly studies also have established the same fact (Ch et al. 2020; Mehta and Singh 2013; Tiwari et al. 2016; Meena et al. 2020; Iqbal and Beigh 2017; Sarmah et al. 2017; Chatterjee et al. 2019). Moreover, the results have shown that users usually reveal their details on various sites. Hence, this acts as a catalyst for increasing cybercrimes since criminals can access personal information. Hence, it is not safe to put personal information on social networking sites as there is a possibility of misuse.

The study has revealed further reasons, including lack of computer literacy, ignorance about cyber laws, unemployment of educated youth, and lower conviction rate for cybercrimes, as some of the subsidiary reasons for the increase in such crimes. The results have shown that slightly less than 20% of the respondents claimed lack of computer literacy to be one of the prominent reasons for cybercrimes. In this age of technology, this is such a contentious issue. Since individuals are so much dependent on technology, the level of computer literacy should be quite higher as well. Awareness of various cyber laws would also prevent women from being victims of various cybercrimes.

Moreover, unemployed educated youth is a prime reason for the increase in cybercrimes. The lack of job opportunities in a heavily populated country such as India leaves the educated youth without an opportunity to secure their livelihood. Hence, some of them get involved in cybercrimes.

Evaluating the impact of cybercrimes on victims, especially women, is also essential. Chaudhary (2019) has cited psychological reasons behind the surge in cybercrimes. She has highlighted that women are often isolated from the mainstream society, and they try to indulge in interactions with strangers in chat rooms and thus become vulnerable to cybercrimes. The study has presented similar findings where 69.9% of the victims say that cybercrime has affected them psychologically. The psychological effects included a desire to take revenge, anger issues, fear, and panic.

Scholars (Bates 2017; Halder and Jaishankar 2014) have documented that females encountering online sexual violence undergo tremendous embarrassment. Backe et al. (2018) and the United Nations Human Rights Office of the High Commissioner (2017) have stated that cyber violence places the survivor in serious mental, physical, and sexual agony. Moreover, it has a tremendous impact on a person's cultural and social values. Various symptoms are experienced among the survivors due to the cyber violence they experienced (United Nations Human Rights Office of the High Commissioner 2017; Madkour et al. 2014; Park et al. 2018). Issues of anxiety and depression are possibilities for cyber violence victims (Haynie et al. 2013). Cyber violence also affects their physical condition such as weight loss. Scholarly studies have also revealed that experiences of ostracization and shame are some of the common outcomes of cyber violence (Button and Miller 2013; Gillett 2018; Madkour et al. 2014). The findings have revealed that to primarily increase the reporting of cybercrime cases, it is necessary to educate women regarding cyber security laws and stop blaming the victim. Higher awareness of cybercrimes also helps women come forward and report the crime, which can lead to the legal punishment of the offender, and a safer and friendlier environment for women in cyberspace. In Indian society, victims are still shamed for being subjected to harassment instead of receiving counselling.

Other than the acute psychological issues faced by the victims, cyber violence creates a kind of social hegemony that prohibits women and girls from raising their voices against cybercrimes. Various other vulnerable groups are also unable to raise their voices against cybercrimes (Powell and Henry, 2017). Moreover, cyber violence can cause withdrawal from online space and self-harm (van Laer 2014). Additionally, online sexual harassment can have a serious degree of impact on the economic and employment life of the victim. Prospective employers may refuse employment based on the online history of a person (Citron 2014). It is worth mentioning that the types of social, economic, and psychological impacts on the victims as a result of the cybercrimes have also created a climate of fear and apprehension among the victims. The male dominance and patriarchal systems of the internet are among the prime factors for increase in cybercrimes.

This study, however, has its limitations. The current pandemic restricted mobility and reaching out to respondents to conduct face-to-face interviews was not possible. The respondents might have misinterpreted the questions because of the lack of guidance while answering each question. Moreover, the research included respondents from the age groups of 16 to 25 and 26 to 35 years, so the study did not focus on women above 35 years of age. Hence, drawing generalisations for individuals aged above than 35 is challenging. Furthermore, the study only relied on the victims' responses, not the offenders.

RECOMMENDATIONS AND POLICY SUGGESTIONS

Awareness and Education: Mehta and Singh (2013) have identified lower awareness levels for the surge in cybercrimes. Studies have advocated the issue of creating awareness regarding cyberspace and diverse forms of cybercrimes among the citizens (Kaur 2015; Tiwari et al. 2016). Facilitating an environment to ensure digital literacy for women and girls can overcome the gender gap in internet usage. Moreover, the educational institutions must organise webinars, workshops, and seminars to spread awareness of digital safety and encourage every individual to report the crimes to fight against the cybercrimes. It is necessary to educate both the parents and students on safe surfing. Furthermore, awareness can be created among women and girls about the penal provisions that exist to protect from online abuse and use the internet cautiously.

Inclusive Approach: Women have been systematically excluded from all the sectors and are historically marginalised. Moreover, women are treated as inferior compared to their male counterparts (Chaudhary 2019). There are very few instances where women are involved in policy-making exercises. Inclusion of more women into the cyber security workforce will help to produce gender-neutral technology and policies.

Enhancing Digital Infrastructure and Robust Legislation: Kundi et al. (2014) has advocated the need for a competent legal framework to deal with cybercrimes. Scholarly studies have pressed the need for a strict approach to dealing with cybercriminals and developing a mechanism to criminalise various forms of cybercrimes (Kaur 2015; Hassan et al. 2020).

Deployment of Adequate Cybersecurity Professionals: The deployment of more cyber security experts and training of the existing staff with the help of new emerging tools used to find the criminals is indispensable to punish the perpetrators of the crime.

Development of a Social Strategy: Considering the nature and degree of cybercrimes against women and girls, there is a need to devise a social strategy involving four prominent elements, namely 1) Learn, 2) Unlearn, 3) Adapt, and 4) Execute. "Learn" is to educate women in the form of awareness campaigns to teach people how not to misuse the internet and why it is important not to misuse it. "Unlearn" is the need to be unlearnt about the objectification of a particular gender by treating them as inferiors. Doing this could also intensify the notion of gender equality in Indian society. "Adapt" is to teach people to adapt to the emerging technologies as the recent COVID-19 pandemic has led to an increase in virtual interactions. The use of the internet by every single individual has become a prerequisite. Hence, it is necessary to develop mechanisms to ensure that cyberspace becomes a secure and safe place for people of all genders. "Execute" is the most vital step to execute necessary steps to curb any violence in cyberspace on a massive scale.

CONCLUSION

Overall, it is found that awareness about cybercrimes is minimal (Poulpunitha et al. 2020). Scholarly studies have identified a lack of awareness as a prime factor behind the escalation in cybercrimes (Kandpal and Singh 2013; Anisha 2017; Ch et al. 2020; Singh 2018). The information collected from the respondents substantiates the same proposition that the lack of education and lack of awareness of cyber security issues and cybercrimes are the prime factors leading to the surge of the cybercrimes.

Historically, women have been subjected to various forms of discrimination (Sethi and Pradhan 2012) and crimes, the newest being cybercrimes. It has been discussed earlier that many cybercrime cases go unreported in India (Jain 2017). Women are prone to victim-blaming, the result of which the majority of them prefer to maintain silence over the cybercrimes committed against them. Most women and girls block or ignore the hateful, vengeful, and sexual messages instead of reporting them. Moreover, the anonymity of the offender acts as a barrier for the victims from reporting. In addition to that, the non-availability of strict laws to curb cyberviolence and the deficiency of cyber cells across India to investigate cybercrimes add to the woes of women and girls who are victims of cybercrimes.

Results exhibit that computer literacy is higher among males than females (Sangwan 2019), which has attributed to women's higher vulnerability to cybercrimes. Chaudhary (2019), in her study, has also highlighted the issues of computer illiteracy among women and how it makes women fall prey to various cybercrimes. She has also cited reasons of easy accessibility and addiction as primary reasons.

Each woman is likely to face cyber violence irrespective of their time on the internet. Hence, it is imperative to analyse the effect of violence on the victim. The fear of victim-blaming and isolation looms large in the victim's thought process, which explains why many cases go unreported. Moreover, in the guise of family honour, many cases are suppressed. The suppression of cybercrimes affects the victim psychologically through depression, fear, anxiety, and withdrawal from cyberspace. To overcome these kinds of effects, victims often share the situation they have faced with friends, close acquaintances, and family members.

NOTES

* Dr Subhra Rajat Balabantaray has completed M.A. (Sociology), M.Phil. (Sociology) from Pondicherry University, and PhD (Sociology) from University of Hyderabad. He has worked in the capacity of Project Fellow, Research Associate and Field Investigator in multiple research projects. He has also worked as a Consultant for London School of Economics. He has been working in the School of Business (University of Petroleum and Energy Studies) for the past six years. He has published several research papers in various journals. His research interests include sociology of development, sociology of environment, and gender studies.

** Mausumi Mishra has completed her M.A. and M.Phil. in Sociology from Centre for the Study of Social Systems (CSSS), Jawaharlal Nehru University (JNU) and is currently pursuing her PhD. She has experience in working with different national and international bodies concerning women centric issues and discrimination. She has been teaching in the Department of Sociology, Wilson College, Mumbai.

*** Upananda Pani completed his M.A. (Economics), M.Phil. (Economics) from the University of Hyderabad, University Grants Commission (UGC) National Eligibility Test (NET). He has worked as a research fellow (Indian Institute of Technology, Khargpur), and is currently pursuing his PhD from the Gokhale Institute of Politics and Economics. He has worked in the analytics industry for four years. He has also worked as a consultant to the Department for International Development (DFID), India for project evaluation. Overall, he has four years of industry experience and eight years of academic experience teaching in University of Petroleum and Energy Studies. He has presented and published several research papers analysing crude derivative markets and natural gas derivative markets on the Indian market. He has published several papers in national and international journals. His research interest includes computational economics, derivative markets, and risk management, open source computing and social media analytics. His area of interest includes financial economics, applied econometrics and energy trading and risk management.

REFERENCES

Agarwal, N. and Kaushik, N. 2014. Cybercrimes against women. *Global Journal of Research in Management* 4 (1): 37–49.

Ahmed, S., Kabir, A., Sneha, S. S. A. and Jafrin, S. 2017. Cyber-crimes against womenfolk on social networks: Bangladesh context. *International Journal of Computer Applications* 174 (4): 9–15. https://doi.org/10.5120/ijca2017915407

Alamo, T., Reina, D. G., Mammarella, M. and Abella, A. 2020. Covid-19: Open-data resources for monitoring, modeling, and forecasting the epidemic. *Electronics* 9 (5): 827. https://doi.org/10.3390/electronics9050827

Anisha. 2017. Awareness and strategy to prevent cybercrimes: An Indian perspective. *Indian Journal of Applied Research* 7 (4): 114–116. https://doi.org/10.36106/ijar

Backe, E. L., Lilleston, P. and McCleary-Sills, J. 2018. Networked individuals, gendered violence: A literature review of cyberviolence. *Violence and Gender* 5 (3): 135–146. https://doi.org/10.1089/vio.2017.0056

Banerjee, S. and Singh, A. 2021. Media sensitivity towards cybercrimes against women. *Indian Journal of Gender Studies* 28 (3): 453–461. https://doi.org/10.1177/09715215211030543

Barik, K., Konar, K., Banerjee, A., Das, S. and Abirami, A. 2022. Analysis and forecasting of cybercrime incident in India. In *ICT systems and sustainability. Lecture notes in networks and systems, vol 321*, eds. Tuba, M., Akashe, S. and Joshi, A., 691–701. Singapore: Springer. https://doi.org/10.1007/978-981-16-5987-4_70

Barker, K. and Jurasz, O. 2019. Online misogyny: A challenge for digital feminism? *Journal of International Affairs* 72 (2): 95–114.

Bates, S. 2017. Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors. *Feminist Criminology* 12 (1): 22–42. https://doi.org/10.1177/1557085116654565

Button, D. M. and Miller, S. L. 2013. Teen dating relationships and outcomes of well-being: Examining gender differences in nonviolent and violent dating relationships. *Women & Criminal Justice* 23 (3): 247–265. https://doi.org/10.1080/08974454.2013.806839

Castiglione, A., Colace, F., Moscato, V. and Palmieri, F. 2018. CHIS: A big data infrastructure to manage digital cultural items. *Future Generation Computer Systems* 86: 1134–1145. https://doi.org/10.1016/j.future.2017.04.006

Ch, R., Gadekallu, T. R., Abidi, M. H. and Al-Ahmari, A. 2020. Computational system to classify cybercrime offenses using machine learning. *Sustainability* 12 (10): 4087. https://doi.org/10.3390/su12104087

Chakraborty, C., Afreen, A. and Pal, D. 2021. Crime against women in India: A state level analysis. *Journal of International Women's Studies* 22 (5): 1–18.

Chatterjee, S., Kar, A. K., Dwivedi, Y. K. and Kizgin, H. 2019. Prevention of cybercrimes in smart cities in India: From a citizen's perspective. *Information Technology & People* 32 (5): 53–83. https://doi.org/10.1108/ITP-05-2018-0251

Chaudhary, V. 2019. Cyber crime against women. *Chetana: International Journal of Education* 4 (1): 116–125.

Chudasama, D., Patel, D., Shah, A. and Shaikh, N. 2020. Research on cybercrime and its policing. *American Journal of Computer Science and Engineering Survey* 8 (3): 14.

Chudasama, D. and Solanki, L. 2021. Cyber crimes and challenges faced by criminal justice system. *International Journal of Information Security and Software Engineering* 7 (1): 6–12.

Citron, D. K. 2014. *Hate crimes in cyberspace*. Cambridge, MA: Harvard University Press. https://doi.org/10.4159/harvard.9780674735613

Dalla, H. S. and Geeta. 2013. Cybercrimes: A threat to persons, properties, governments and societies. *International Journal of Advanced Research in Computer Science and Software Engineering* 3 (5): 997–1002.

Datta, P., Panda, S. N., Tanwar, S. and Kaushal, R. K. 2020. A technical review report on cyber crimes in India. In *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)*, 12–14 March 2020, Pune, India, eds. Datta, P., Panda, S. N., Tanwar, S. and Kaushal, R. K., 269–275. Piscataway, NJ: Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/ESCI48226.2020.9167567

Deora, R. S. and Chudasama, D. 2021. Brief study of cybercrime on an internet. *Journal of Communication Engineering & Systems* 11 (1): 1–6.

Dogra, B. and Kalra, R. 2018. The reality of virtual threats against women in India. *International Journal of Research in Social Sciences* 8 (12): 312–325.

Dhapola, S. 2020. How the internet kept India moving despite the pandemic. *The Indian Express*, 31 December 2020. https://indianexpress.com/article/technology/tech-news-technology/how-the-internet-kept-india-moving-despite-the-pandemic-7127335/ (accessed 15 September 2021).

Elavarasi, M. 2021. Analysis of cybercrime investigation mechanism and counsel of defense in India. *Turkish Journal of Computer and Mathematics Education* 12 (13): 682–684.

Gillett, R. 2018. Intimate intrusions online: Studying the normalisation of abuse in dating apps. *Women's Studies International Forum* 69: 212–219. https://doi.org/10.1016/j.wsif.2018.04.005

Goyal, M. 2012. Ethics and cyber crime in India. *International Journal of Engineering and Management Research* 2 (1): 1–3.

Gupta, A. 2014. *Reporting and incidence of violence against women in India*. New Delhi: Rice Institute.

Hadi, A. 2017. Patriarchy and gender-based violence in Pakistan. *European Journal of Social Science Education and Research* 4 (4): 289–296. https://doi.org/10.26417/ejser.v10i2.p297-304

Halder, D. 2017a. Revenge porn against women and the applicability of therapeutic jurisprudence: A comparative analysis of regulations in India, Pakistan, and Bangladesh. In *Therapeutic jurisprudence and overcoming violence against women*, eds. Halder, D. and Jaishankar, K., 282–292. New Delhi: IGI Global. https://doi.org/10.4018/978-1-5225-2472-4.ch017

____. 2017b. Criminalising revenge porn from the privacy aspects: The model revenge porn prohibitory provision. *Live Law*, 15 September 2017. https://www.livelaw.in/criminalizing-revenge-porn-privacy-aspects-model-revenge-porn-prohibitory-provision/?infinitescroll=1 (accessed 9 November 2021).

____. 2015. Cyber stalking victimisation of women: Evaluating the effectiveness of current laws in India from restorative justice and therapeutic jurisprudential perspectives. *Temida* 18 (3–4): 103–130. https://doi.org/10.2298/TEM1504103H

Halder, D. and Jaishankar, K. 2016. *Cybercrimes against women in India*. New Delhi: SAGE Publications.

____. 2014. Patterns of sexual victimization of children and women in the multipurpose social networking sites. In *Social networking as a criminal enterprise*, eds. Marcum, C. D. and Higgins, G. E., 124–144. Boca Raton, FL: Routledge.

____. 2011. Cyber gender harassment and secondary victimization: A comparative analysis of the United States, the UK, and India. *Victims & Offenders* 6 (4): 386–398. https://doi.org/10.1080/15564886.2011.607402

____. 2009. Cyber socializing and victimization of women. *Temida* 12 (3): 5–26. https://doi.org/10.2298/TEM0903005H

Hassan, F. M., Khalifa, F. N., El Desouky, E. D., Salem, M. R. and Ali, M. M. 2020. Cyber violence pattern and related factors: Online survey of females in Egypt. *Egyptian Journal of Forensic Sciences* 10: 6. https://doi.org/10.1186/s41935-020-0180-0

Haynie, D. L., Farhat, T., Brooks-Russell, A., Wang, J., Barbieri, B. and Iannotti, R. J. 2013. Dating violence perpetration and victimization among U.S. adolescents: Prevalence, patterns, and associations with health complaints and substance use. *Journal of Adolescent Health* 53 (2): 194–201. https://doi.org/10.1016/j.jadohealth.2013.02.008

Iqbal, J. and Beigh, B. M. 2017. Cybercrime in India: Trends and challenges. *International Journal of Innovations & Advancement in Computer Science* 6 (12): 187–196.

Jain, M. 2017. Victimization of women beneath cyberspace in Indian upbringing. *Bharati Law Review* 1 (1): 1–11.

Jain, O., Gupta, M., Satam, S. and Panda, S. 2020. Has the COVID-19 pandemic affected the susceptibility to cyberbullying in India? *Computers in Human Behavior Reports* 2: 100029. https://doi.org/10.1016/j.chbr.2020.100029

Joshi, Y. and Singh, A. 2013. A study on cyber crime and security scenario in India. *International Journal of Engineering and Management Research* 3 (3): 13–18.

Kandpal, V. and Singh, R. K. 2013. Latest face of cybercrime and its face in India. *International Journal of Basic and Applied Sciences* 2 (4): 150–156.

Kaphle, P. 2019. Cyber violence against women and girls in Nepal. *Kathmandu School of Law Review* 7 (1): 85–99.

Kashyap, S. and Chand, K. 2020. History of cyber crimes: Facts which are still unknown. *The International Journal of Analytical and Experimental Modal Analysis* 12 (10): 134–138.

Kaur, R. 2015. Cybercrimes against women: Present scenario. *International Journal in Management and Social Science* 3 (9): 233–241.

Khudhair, N. S. 2021. Competence in cybercrime: A review of existing laws. *Revista Geintec-Gestao Inovacao e Tecnologias* 11 (4): 1950–1969.

Kethineni, S. 2020. Cybercrime in India: Laws, regulations, and enforcement mechanisms. In *The Palgrave handbook of international cybercrime and cyberdeviance*, eds. Holt, T. and Bossler, A., 305–326. London: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3_7

Kshetri, N. 2016. Cybercrime and cybersecurity in India: Causes, consequences and implications for the future. *Crime, Law and Social Change* 66 (3): 313–338. https://doi.org/10.1007/s10611-016-9629-3

Kundi, G. M., Nawaz, A. and Akhtar, R. 2014. Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries. *Journal of Information Engineering and Applications* 4 (4): 61–70.

Luong, H. T., Phan, H. D., Chu, D. V., Nguyen, V. Q., Le, K. T. and Hoang, L. T. 2019. Understanding cybercrimes in Vietnam: From leading-point provisions to legislative system and law enforcement. *International Journal of Cyber Criminology* 13 (2): 290–308. https://doi.org/10.5281/zenodo.3700724

Madkour, A. S., Xie, Y. and Harville, E. W. 2014. Pre-pregnancy dating violence and birth outcomes among adolescent mothers in a national sample. *Journal of Interpersonal Violence* 29 (10): 1894–1913. https://doi.org/10.1177/0886260513511699

Malar, M. N. 2012. Impact of cyber crimes on social networking pattern of girls. *International Journal of Internet of Things* 1 (1): 9–15. https://doi.org/10.5923/j.ijit.20120101.02

Mansi and Agarwal, P. 2020. Cybercrime: Women combating with the negative effect of technology in the era of globalization. *International Journal of Management and Humanities* 4 (7): 21–25. https://doi.org/10.35940/ijmh.F0650.034720

Meena, Y., Sankhla, M. S., Mohril, S. and Kumar, R. 2020. Cybercrime: Youth awareness survey in Delhi NCR, India. *Forensic Research & Criminology International Journal* 8 (5): 177–180. https://doi.org/10.15406/frcij.2020.08.00325

Mehta, S. and Singh, V. 2013. A study of awareness about cyberlaws in the Indian society. *International Journal of Computing and Business Research* 4 (1): 1–8.

Mondal, D. and Paul, P. 2021. Associations of power relations, wife-beating attitudes, and controlling behavior of husband with domestic violence against women in India: Insights from the National Family Health Survey–4. *Violence Against Women* 27 (14): 2530–2551. https://doi.org/10.1177/1077801220978794

Nappinai, N. S. 2010. Cyber crime law in India: Has law kept pace with emerging trends? An empirical study. *Journal of International Commercial Law and Technology* 5 (1): 22–28.

National Crime Records Bureau (NCRB). 2022. Crime in India table contents. https://ncrb.gov.in/en/crime-in-india-table-addtional-table-and-chapter-contents?page=27 (accessed 20 September 2022).

Ompal, Pandey, T. and Alam, B. 2017. How to report cyber crimes in Indian territory. In *International Conference on Emerging Trends in Engineering, Technology, Science and Management*, 12 April 2017, IIMT College of Engineering, Greater Noida, India, 5–19.

Pajankar, S. 2020. Cyber crimes and cyber laws in India. *Delta National Journal of Multidisciplinary Research* 7 (1): 25–29.

Panwar, K. and Sihag, V. K. 2020. Changing forms of cyber violence against women and girls. *The Indian Police Journal* 67 (4): 111–120.

Park, Y., Mulford, C. and Blachman-Demner, D. 2018. The acute and chronic impact of adolescent dating violence: A public health perspective. In *Adolescent dating violence: Theory, research and prevention*, eds. Wolfe, D. A. and Temple, J. R., 53–83. Cambridge, MA: Academic Press. https://doi.org/10.1016/B978-0-12-811797-2.00003-7

Pawar, M. U. and Sakure, A. 2019. Cyberspace and women: A research. *International Journal of Engineering and Advanced Technology* 8 (6S3): 1670–1675. https://doi.org/10.35940/ijeat.F1313.0986S319

Pogge, T. and Sengupta, M. 2015. The Sustainable Development Goals (SDGS) as drafted: Nice idea, poor execution. *Washington International Law Journal* 24 (3): 571–587.

Poulpunitha, S., Manimekalai, K. and Veeramani, P. 2020. Strategies to prevent and control of cybercrime against women and girls. *International Journal of Innovative Technology and Exploring Engineering* 9 (3): 609–612. https://doi.org/10.35940/ijitee.K2408.019320

Powell, A. and Henry, N. 2017. *Sexual violence in a digital age*. London: Palgrave Macmillan. https://doi.org/10.1057/978-1-137-58047-4

Ökten, Ş. 2017. Domestic violence and patriarchy in Turkey. *European Journal of Social Science Education and Research* 4 (4s): 365–369. https://doi.org/10.26417/ejser.v11i2.p365-369

Rao, Y. S., Rauta, A. K., Saini, H. and Panda, T. C. 2016. Influence of educational qualification on different types of cybercrime: A statistical interpretation. *Indian Journal of Science and Technology* 9 (32). 1–7. https://doi.org/10.17485/ijst/2016/v9i32/100189

Ravindran, S. and Shah, M. 2020. Covid-19: 'Shadow pandemic' and violence against women. *Ideas for India*, 17 September 2020. https://www.ideasforindia.in/topics/poverty-inequality/covid-19-shadow-pandemic-and-violence-against-women.html (accessed 25 October 2021).

Saha, T. and Srivastava, A. 2014. Indian women at risk in the cyberspace: A conceptual model of reasons of victimization. *International Journal of Cyber Criminology* 8 (1): 57–67.

Sangwan, P. 2019. A critical study of violation of women's right in India with special reference to cybercrime. *IME Journal* 13 (2): 148–55. https://doi.org/10.5958/2582-1245.2019.00006.X

Sankhwar, S. and Chaturvedi, A. 2018. Woman harassment in digital space in India. *International Journal of Pure and Applied Mathematics* 118 (20): 595–607.

Saravanan, S. 2000. *Violence against women in India. A literature review*. New Delhi: Institute of Social Studies Trust (ISST).

Sarkar, S. and Rajan, B. 2021. Materiality and discursivity of cyber violence against women in India. *Journal of Creative Communications*. https://doi.org/10.1177/0973258621992273

Sarmah, A., Sarmah, R. and Baruah, A. J. 2017. A brief study on cyber crime and cyber law's of India. *International Research Journal of Engineering and Technology* 4 (6): 1633–1641.

Sawaneh, I. A. 2020. Cybercrimes: Threats, challenges, awareness, and solutions in Sierra Leone. *Asian Journal of Interdisciplinary Research* 3 (1): 185–195. https://doi.org/10.34256/ajir20114

Saxena, P., Kotiyal, B. and Goudar, R. H. 2012. A cyber era approach for building awareness in cyber security for educational system in India. *International Journal of Information and Education Technology* 2 (2): 167–170.

Sethi, N. and Pradhan, H. 2012. Patterns of consumption expenditure in rural households of Western Odisha of India: An Engel ratio analysis. *OIDA International Journal of Sustainable Development* 5 (4): 107–120.

Shan-A-Khuda, M. and Schreuders, C. 2019. Understanding cybercrime victimisation: Modelling the local area variations in routinely collected cybercrime police data using latent class analysis. *International Journal of Cyber Criminology* 13 (2): 493–510.

Sharma, I. and Alam, M. A. 2016. Privacy and freedom issues in cyberspace with reference to cyber law. *International Journal of Computer Applications* 145 (3): 11–18. https://doi.org/10.5120/ijca2016910185

Sikweyiya, Y., Addo-Lartey, A. A., Alangea, D. O., Dako-Gyeke, P., Chirwa, E. D., Coker-Appiah, D., Adanu, R. M. K. and Jewkes, R. 2020. Patriarchy and gender-inequitable attitudes as drivers of intimate partner violence against women in the central region of Ghana. *BMC Public Health* 20: 682. https://doi.org/10.1186/s12889-020-08825-z

Singh, J. 2015.Violence against women in cyber world: A special reference to India. *International Journal of Advanced Research in Management and Social Sciences* 4 (1): 60–76.

Singh, P. 2018. Cyber crime against women in India. PhD diss., Banaras Hindu University, India.

Singh, R., Singh, P. and Parveen, F. 2014. Cyber crimes: The rampaging threat. *International Journal of Research in Information Technology* 2 (12): 86–93.

Sobieraj, S. 2018. Bitch, slut, skank, cunt: Patterned resistance to women's visibility in digital publics. *Information, Communication & Society* 21 (11): 1700–1714.

Srivastava, A. and Yadav, S. 2014. Cyber stalking: A nuisance to the information technology. *International Journal of Advanced Research in Computer Science* 5 (8): 98–100.

Tiwari, S., Rawat, A. and Bhalla, R. 2016. Cybercrime and security. *International Journal of Advanced Research in Computer Science and Software Engineering* 6 (4): 46–52.

United Nations Human Rights Office of the High Commissioner. 2017. UN experts urge States and companies to address online gender-based abuse but warn against censorship. https://www.ohchr.org/en/press-releases/2017/03/un-experts-urge-states-and-companies-address-online-gender-based-abuse-warn (accessed 15 October 2021).

van Laer, T. 2014. The means to justify the end: Combatting cyber harassment in social media. *Journal of Business Ethics* 123: 85–98. https://doi.org/10.1007/s10551-013-1806-z

Varalakshmi, R. 2020. Digital steganography for preventing cybercrime using artificial intelligence technology. *Journal of Critical Reviews* 7 (6): 749–753.

Viraja, V. K. and Purandare, P. 2021. A qualitative research on the impact and challenges of cybercrimes. *Journal of Physics: Conference Series* 1964: 042004. https://doi.org/10.1088/1742-6596/1964/4/042004

Visaria, L. 2008. Violence against women in India: Is empowerment a protective factor? *Economic and Political Weekly* 43 (48): 60–66.

Wadhwa, A. and Arora, N. 2017. A review on cybercrime: Major threats and solutions. *International Journal of Advanced Research in Computer Science* 8 (5): 2217–2221.

Waware, P. 2018. Review on cybercrime: Threats and preventions. *International Research Journal of Engineering and Technology* 5 (11): 1576–1578.

Yadav, H., Gautam, S., Rana, A., Bhardwaj, J. and Tyagi, N. 2021. Various types of cybercrime and its affected area. In *Emerging technologies in data mining and information security*, eds. Tavares, J. M. R. S., Chakrabarti, S., Bhattacharya, A. and Ghatak, S., 305–315. Singapore: Springer. https://doi.org/10.1007/978-981-15-9774-9_30

Yar, M. and Drew, J. M. 2019. Image-based abuse, non-consensual pornography, revenge porn: A study of criminalization and crime prevention in Australia and England & Wales. *International Journal of Cyber Criminology* 13 (2): 578–594.

Yasin, A, Fatima, R., Liu, L., Wang, J. Ali, R. and Wei, Z. 2021. Understanding and deciphering of social engineering attack scenarios. *Security and Privacy* 4 (4): e161. https://doi.org/10.1002/spy2.161

Zahoor, R. and Razi, N. 2020. Cyber-crimes and cyber laws of Pakistan: An overview. *Progressive Research Journal of Arts and Humanities* 2 (2): 133–143. https://doi.org/10.51872/prjah.vol2.Iss2.43