INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Aug 2023

ISSN: 2582-6433

FAKE ACCOUNT VICTIMIZATION: AN EMPIRICAL RESEARCH IN SONIPAT AREA

AUTHORED BY: CHHAVI JAIN & TANYA MITTAL
COURSE: LLB (Hons) 2nd Year
SRM UNIVERSITY, DELHI NCR
MAIL ID: jainchhavu00@gmail.com, tanyamittal@gmail.com

ABSTRACT

Today's world is a technological world as the number of online platform users is increasing rapidly. These platforms are Facebook with 2.9 billion users globally and 2.96 million users from India, YouTube with 2.5 billion users globally and 467 million Indian users, WhatsApp with 2 billion users globally and 487.5 million Indian users and Instagram with 2 billion users globally and 229 million users are Indian.

The number of users has increased rapidly from 970 million in 2010 to 4.76 billion in January 2023, sothe crime rate through these platforms is also taking a plight. Criminal activities like cyberbullying, cyberstalking, and profile hacking through fake social media accounts have become the most common problem, especially for women. Statistics show that out of the total users of Facebook and Instagram, 5% of accounts are fake and Womenare easy targets for any anonymous person on these platforms. This paper shall analyse the problems, women face due to these dummy accounts with the help of an empirical research methodology in the area of Sonipat, Haryana. The researchers also attempt to try to find out solutions to tackle this very problem with the help of government policies and relevant laws.

ISSN: 2582-6433

SYNOPSIS

1. INTRODUCTION

Today's world can be called a digital world, where people are more connected with each other through digital sources rather than personal interaction. Social media platforms have emerged as a major contributor and the digitalization of today's world. The most commonly used social media platforms are Facebook, YouTube, WhatsApp, Twitter, and Instagram. These platforms provide various types of facilities to their users, starting from communication with other users to the opportunity for exchanging views and ideas, from sharing valuable information to the current news about the latest event, these platforms have ultimately evolved as a source of entertainment for today's generation. The figure of users on social media platforms is growing rapidly. At present, more than 50% of the world's population, i.e., around 59%, uses social media platforms. As per the data provided by the team Kepios, in April 2023, the active number of users on social media platforms was 4.80 billion[1].

It is expected that globally there will be 5.85 billion users on social media platforms in 2027[2], and 1177.5 million users will be from India[3]. This shows how much the use of social media platforms has increased. Moreover, excessive use of anything always creates trouble, so as in the case of these platforms, with the rapid increase in usage, wastage of time, crime rate, etc., is also on the rise. Data provided by GWI shows that a social media user actively spends an average of 2 hours and 24 minutes per day using social media[4].

The most used platform among all is Facebook globally with 2.9 billion users[5], but in India, WhatsApp is the most popular with 487.5 million users[6].

[1]Global Social Media Statistics, *available at*: https://datareportal.com/social-media-users#:~:text (last visited on April 30, 2023).
[2]Number of global social network users 2017-2027, *available at:*https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (last visited on April 29, 2023).
[3]Number of social network users India 2015-2040, *available at:* https://www.statista.com/statistics/278407/number-of-social-network-users-in-india/ (last visited on April 29, 2023).
[4]*Supra* note 1.
[5] Global social networks ranked by number of users 2023, *available at:* https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/(last visited on April30, 2023).
[6] WhatsApp statistics 2023, *available at:*https://www.demandsage.com/whatsapp-statistics/ (last visited on April 30, 2023).

ISSN: 2582-6433

The speedygrowth in the number of users may be because these platforms provide almost all of the information required to stay current in daily life. Information regarding jobs, entertainment, news, newly launched products, etc. is easily accessible, and with the help of these platforms, one can connect with a large number of people the most probable reason is that every facility is available in one place. There is no need to go anywhere to earn a living too, Individuals can earn by posting content on these platforms, and they can also get fame very easily within no time.

Though social media platforms have numerous potential benefits it is well said that every coin has two sides. Despite its positive use, it also has a negative impact. People are becoming addicted to it, especially our young generation, which creates severe problems in their lives such as distraction, disrupting sleep, spreading rumours, depression, and so on. Moreover, a breach of privacy is a major concern. Also, a plethora of new types of crimes is emerging through it, like online fraud, scams, defamation, etc. As per the data from the "National Crime Record Bureau", as of 2019, the overall number of cybercrime occurrences increased by 18.4%, and the proportion of cases involving women increased by 28%[7].

Women are the easiest target for an anonymous person. Cyber blackmail, threats, cyber pornography, publishing and sending obscene sexual content, stalking, bullying, defamation, morphing, and creating phoney profiles are the most prevalent cybercrimes against women. According to the report of the National Crime Record Bureau, cybercrime against women has gone up by 28% in 2019. 10,730 events out of the 52,974 incidents of cybercrime recorded in 2021 were crimes against women[8].

People often use fake social media accounts to commit these crimes and to satisfy their evil desires. The practice of creating fake social media accounts is one of the contemporary issues. Every day, thousands of phoney social media profiles are created by scammers, fraudsters, hackers, and wicked individuals. Everyone can be a target, including famous people, influential people, and even a common person. Facebook dealt with 1.6 billion bogus accounts in the first quarter of 2022[9]. Over 10

[7] Anoushka Sawhney,"Cybercrime against women up 28% since 2019:Karnataka's share highest: NCRB", *Business Standard*, August 30, 2022, available at<https://www.business-standard.com/article/current-affairs/cybercrime-against-women-up-28-since-2019-national-crime-records-bureau-122083001139_1.html> (last visited on May 16, 2023).
[8] *Supra* note 7.
[9] Facebook: fake account removal as of Q4 2022, *available at:*

ISSN: 2582-6433

bot accounts are deleted by Twitter every second, for a total of over 310 million every year. An estimated 95 million Instagram accounts are phoney, with an estimated 1 billion users. It means 1 in 10 Instagram accounts are fake[10]. Fake profiles are used to commit cybercrimes with an unknown identity. Cybercrimes include cyberbullying, online stalking, and misuse of someone's data like photos, videos, etc. Among these crimes, the most targeted victims are women.

There are certain provisions provided under the "Indian Penal Code 1860"[11] and the "Information Technology Act, 2000"[12], to control the offences through fake accounts, like under Sections 66C[13] and 66D[14] of the IT Act, 2000[15], where making fake profiles by using fake information, photos, or identity of another person is an offence. The right to privacy is also a fundamental right under "Article 21"[16] of the Indian Constitution.

The laws that are regulating cybercrimes through fake accounts are not very effective. No specific provision is provided under the IT Act, of 2000[17], which deals with cybercrimes against women in particular. There is no special regulatory policy for cybersecurity. There is a lack of awareness among the people regarding these laws, and due to this, most of the cases remain unregistered. Only in the presence of a regulated and overseen legislative framework can users defend themselves and receive protection from cyberattacks.

This study centres on the problem that women face as a result of fake social media accounts. In this research paper, women from both urban and rural areas of Sonipat district (Haryana) are covered.

Researchers will use this research to try to find some suitable solutions to the varied problems. It will also be explored how to reduce the legal gap.

---

https://www.statista.com/statistics/1013474/facebook-fake-account-removal-quarter/#:~:text(last visited on April 30, 2023).

[10]How to identify Fake Instagram followers, *available at*: https://blog.kicksta.co/how-to-identify-fake-instagram-followers-put-a-stop-to-them/#:~:text(last visited on May 16, 2023).

[11] The Indian Penal Code, 1860 (Act 45 of 1860).

[12] The Information Technology Act, 2000 (Act 21 of 2000).

[13]The Information Technology Act, 2000 (Act 21 of 2000), s. 66C.

[14] The Information Technology Act, 2000 (Act 21 of 2000), s. 66D.

[15]*Supra* note 12.

[16] The Constitution of India, art. 21.

[17]*Supra* note 12.

ISSN: 2582-6433

1.1 STATEMENT OF PROBLEM

As discussed above, social media, with its positive uses, also has many negative uses. Youngsters are not only becoming addicted to it, but they are also finding new ways to commit crimes, to upset other people. The offenders are using fake profiles to commit fraud, extort money from people, tease someone, harass someone, etc. On these platforms, the privacy of an individual is not safe. One can misuse the personal information of a person by using his or her pictures, messages, videos, etc.

Threats, bullying, harassment, and stalking of others on social media are the offences that are most frequently reported and observed. According to a survey by **UNICEF** in 2019, in 30 nations, 1 in 3 young people claimed to have experienced online bullying (**UNICEF Poll, 2019**[18]). The country with the highest rate of this issue was India, where 37% of parents said their child had experienced it[19]. The victims of these crimes frequently don't know when to notify the police, so most of this type of behaviour goes unpunished or isn't taken seriously. India reported an 18.4% rise in cybercrime in 2021 (52,974 cases), as it was 44,735 in 2019. Among these, 4047 cases were of online banking fraud; 972 cases were associated with cyberstalking or bullying of women; and 149 instances were of a fake profile. According to NCRB, the maximum 60.2% of cybercrimes reported in 2020 were committed for fraud, 6.6% for sexual exploitation, and 4.9% for extortion[20]. In 2021, India recorded almost 13,000 registered cases of fake digital profiles.

According to research, the average number of social media accounts per Gen Z user around the world is 8.5, and India tops the list with 11.5 social media accounts per user[21]. Around 66 million to 88 million Facebook accounts are believed to be false but haven't yet been identified. These fake accounts are mostly used to harass women socially, emotionally, and economically. In 2018, among the total number of cyberbullying cases, girls were bullied 1.3 times more than boys (**Centre for**

[18]UNICEF POLL: More than a third of young people in 30 countries report being a victim of online bullying, *available at:*https://www.unicef.org/serbia/en/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying(last visited on May 20, 2023).
[19] Cyberbullying statistics 2023, *available at*:https://www.singlecare.com/blog/news/cyberbullying-statistics/#:~:text(last visited on May 15, 2023).
[20]Press Trust of India ltd., "India reported 11.8% rise in cybercrime in 2020; 578 incidents of 'fake news on social media': Data" The Times of India, Sep15, 2021.
[21] Social media users in the world- 2023 demographics, *available at:*https://www.demandsage.com/social-media-users/(last visited on May 16, 2023).

ISSN: 2582-6433

Disease Control, 2019)[22]. Also, in India, out of the total number of reported cases of cyberstalking, 60% of the cases were reported by females.

This is a prevalent concern with the use of social media. This cannot be disregarded by anyone, particularly the women who are the primary victims. Some measures to control this are desperately needed.

In this research, Sonipat district in Haryana state is being studied. The reason for this is that this place is remote from Delhi, the country's capital. Due to its geographic location, it is an intriguing area to research crimes involving fake accounts because it can shed light on the dynamics of such actions close to a significant metropolitan centre. People living in cities close to metropolitan regions are majorly influenced by the lifestyles and habits of those living in metropolitan areas. Due to this influence, crime rates are increasing in this area. Also, the sizeable population of Sonipat makes it possible to find a wide variety of people involved in a variety of activities for illegal operations.

1.2 RESEARCH OBJECTIVE

- Analyse the instances of fake accounts and victimisation of women in India.
- Compare the condition of women in urban and rural areas through empirical research.
- Analyse the effectiveness of the national laws governing the issue.
- Recommend or propose a solution to address the issue.

1.3 RESEARCH METHODOLOGY

With the aid of an empirical research methodology, researchers will analyse the circumstances. Both the urban and rural portions of the Sonipat region in Haryana are the subject of this study. To gather data, Google forms were circulated. Our goal is to gather information from women so that a range of viewpoints can be collected.

We have received almost 160 responses from women, in which participation is equal in urban and rural areas. Based on these responses, researchers will analyse the situation and try to find out the

[22]Government of India, Report: *2019 National and State Healthcare-Associated Infections Progress Report* (Ministry of health and family welfare, 1947).

ISSN: 2582-6433

best way to tackle it.

1.4 CHAPTERIZATION

1. Introduction
2. Analysis of fake accounts in the Sonipat region
3. How women are the main victims?
4. Conditions in urban and rural areas
5. Laws governing the issue of fake accounts in India
6. Solution to tackle crimes through fake accounts
7. Conclusion

2. Analysis of fake accounts in the Sonipat region

As discussed above social media has marked tremendous growth, not only in India but also in the world. The following table expresses the data showing the number of users on different platforms globally as well as in India:

Number of users on Social media platforms[23]

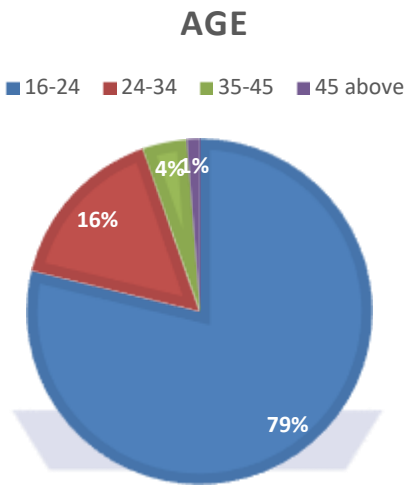
YEAR	GLOBALLY	INDIA
2019	3.51 billion	395.87 million
2020	3.9 billion	518 million
2021	4.26 billion	639.47 million
2022	4.59 billion	755.47 million
2023	4.90 billion	862.08 million
2027(expected)	5.85 billion	1177.5 million

This data talks about the wider section of the world but the researchers will look up and analyse the matter in the Sonipat region from Haryana State.

[23] *Supra* note 2.

ISSN: 2582-6433

The data is gathered from women of various ages, although the number of young women is higher. A total of 170 replies were received, with 134 coming from women aged 16 to 24. This is because social media is more prevalent among young people and has a greater influence on them.



There are various platforms of social media like Facebook, Instagram, YouTube, Twitter, etc. The below-mentioned data indicates that the platforms are very popular among the people.

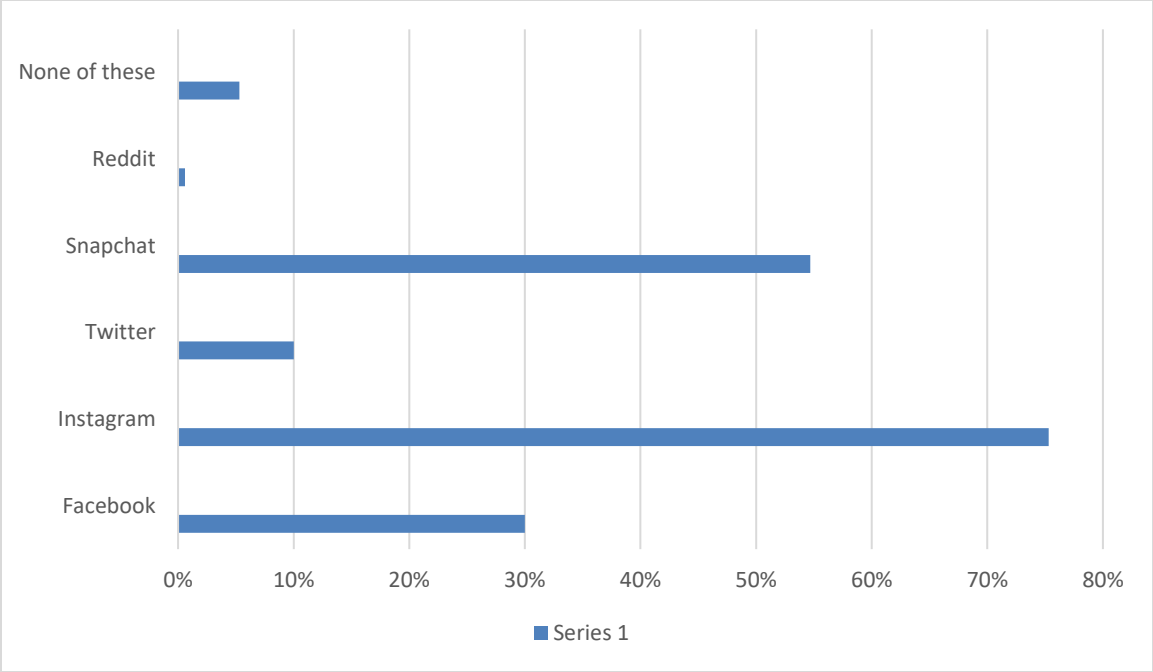
Number of users on different social media platforms in January 2023[24]

NAME OF THE PLATFORM	GLOBALLY	INDIA
Facebook	2.9 billion	314.6 million
YouTube	2.51 billion	467 million
WhatsApp	2 billion	487.5 million
Instagram	2 billion	229.6 million
Snapchat	635 million	172.5 million
Twitter	556 million	27.25 Million

In the research also, almost 92.9% of women have their accounts on social media. The below-mentioned graph indicates the data collected from women in the Sonipat area-:

[24] *Supra* note 5.

ISSN: 2582-6433



As is depicted by the bar graph that 75% of women have accounts on Instagram which shows its popularity among them. Overall data indicates, that more than 95% of women have their accounts on social media, while there are less than 5% of women who don't have an account on these platforms. Now the issue is not about the increasing number of social media accounts but the issue is the increasing number of fake social media accounts. One person is having more than one account on these platforms. The exact number of fake social media accounts is difficult to determine, as the number can vary on different platforms. But experts have suggested that a significant number of social media accounts may be fake. Like, Facebook took action against 1.3 billion fake accounts, in the fourth quarter of 2022[25].

The reasons for creating fake accounts are various and complex, but they often are used for personal gains like deception or manipulation. People create fake accounts to get various information about the targeted user by winning their trust.

Disseminating false information, such as propaganda, fake news, or other misleading information is one of the main reasons behind the bogus accounts. They are also created for spam messages, such as advertisements or scams to the suspect users, in which various websites are attached to the messages

[25] *Supra* note 9.

ISSN: 2582-6433

to get more information. Online frauds are also commonly seen these days which include money fraud by extorting money from innocent people, religious fraud by changing their religion hiding their true identity, etc. Most of these online frauds are done by fake accounts. Nowadays the rate of cybercrime is also increasing, as **National Cyber Crime Reporting Portal** has reported 8, 84,863 complaints from January 2021 to November 2022.

Fake accounts are creating a lot of problems concerning an individual's privacyand the individual's privacy is protected by the Fundamental Rights under Article 21[26]. They enter into their domain with a fake identity or by using someone's identity to earn their trust. So that people can fall into their trap and then they can misuse the trust that provided information.

The target of these fake account users can be a man, woman, child, adult, literate person, illiterate person, or anyone. No one will be spared from their eyes. But the condition of the age group 18-24 years old is more vulnerable because they can be easily targeted. Among them also, women are the main victim. They are facing harassment offline as well as online due to these fraudsters.

3. How women are the main victim?

In India, women are treated as Janni and they are respected as Devi[27]. Still, they have been victims of a range of crimes like Sati Pratha, acid attacks, rape, eve-teasing, sexual harassment, and so on. Even in the recent period, the concerns of women's empowerment have gained popularity due to educational progress and awareness, but on the ground level, women are still considered inferior, face abuse at all stages of life, and deal with a variety of security difficulties.

Current development in science and technology, especially in the Internet and social media, due to which it quite easy for individuals to stay connected. These platforms were created to facilitate communication, social interaction, entertainment, and various carrier opportunities online, which will help in the enhancement of an individual. It is a platform where the businesses can also be promoted.

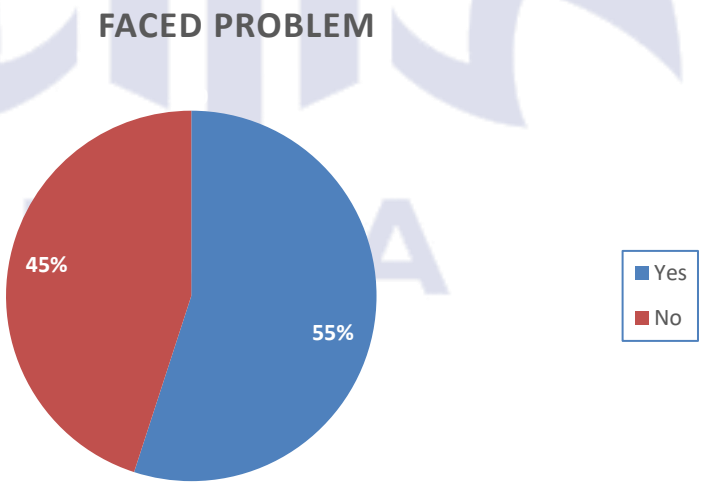
[26] *Supra* note 16.
[27] Saurabh Dubey, "Cyber Crimes and Cyber Laws: A Perspective of Women Victimization"6 *International Journal of Advanced Research in Science, Communication and Technology*(2021).

ISSN: 2582-6433

Hence, these platforms were developed so that they will be useful for individuals but few people know more about how to misuse a thing rather than its positive use. Social media has opened the door for various criminals such as hackers to interfere with the accounts and get unauthorised access to the user's computer system and steal important data. The cyber-world is a virtual environment in which anyone may impersonate or conceal his identity and cause harm to another person.

Nowadays crime against women is a very familiar issue. Every second, one woman is becoming a victim by falling into someone's trap. And between this, these online platforms are now a new area where the privacy, dignity, and security of a woman are being challenged every moment. Technology is there to comfort life but here it has become a mode by which some criminals try to defame a woman by sending her obscene videos and pictures, unstoppable messages, stalking by different – different accounts and worst of them is by creating pornographic videos, which are created without their consent.

In this research, the researchers found that more than 50% of women have faced problems due to fake social media accounts.

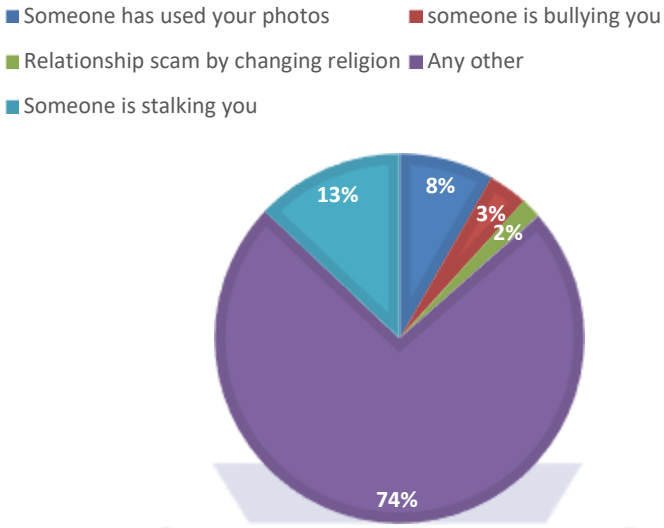


The pie chart shows that almost 55% of women have faced problems due to these fake accounts in the area of Sonipat.

This data is of a confined area, the picture is much larger than one can think. In this confined area, more than half of the women are the victim then we can easily imagine what will be the stats in the whole country and also in the whole world. Actuality, this is a really large and significant problem.

ISSN: 2582-6433

As per the researcher's findings, women have to tackle a lot of problems due to these fake accounts as shown by the pie chart-:



As depicted by the chart there are various kinds of harassment which women had to face due to these fake accounts. Some are-:

- A girl shares her photos with someone she trusts, but that person can be a scammer who is using a phoney account. He can use her images to blackmail her, harass her and force her to do what he wants.
- Fake accounts are created to stalk a girl online. These cases are commonly seen. The account holder is using several accounts just to stalk a girl. If a girl blocks one of his accounts he can again message her with another one.
- With the help of fake accounts the person can make defamatory statements about a woman and can also do sexual comments.
- Cyberbullying is also common these days. The person can abuse the victim online, can make fun of her and humiliate her.
- Recently a new challenge is occurring i.e. with the help of a fake profile the offender can represent a fake religion to trap a girl. In this, the girl falls for him without knowing the true identity of a person and after that, she has to suffer various kind of cruelty and sometimes have to change her religion.

ISSN: 2582-6433

- By creating a false account and using someone else's name, the perpetrator has infringed Article-21[28]- right to privacy of an individual, which is a crime.
- The unstoppable messages even after blocking, hacking of accounts, forcing a girl to get physical with him by using shameless tactics, etc. are some more instances due to which a woman is suffering.

3.1 Women are the main victim but why?

The answer can be varied. Our society is a male dominant society where a man thinks of a woman as his property. He thinks he can control her in the way he wants like mentally, physically, sexually, and emotionally. As of now, society is trying to change this scenario but in a rigid male-male-dominantly it, is difficult for a male to accept that the female is now controlling her own life, they are taking their decisions and they have the **right to say- NO** to a male. If a woman has said no to a man, for example, if a woman is not interested in getting into a relationship with that man, then it hurts his ego of him. In the feeling of taking revenge, due to obsession or attraction, he can do anything just to satisfy his male ego. This is the main reason why Women are the main victims of these accounts.

Another important reason can be that these kinds of crimes remain unreported because for various reasons most women feel hesitation to open up and share what they suffered with anyone or due to a mentality that what will be its impact society, what they think about her, what kind of reaction her family will give, and sometimes she feels that she is responsible to be a victim of such kind of crime. So these are some reasons that in such kinds of crime, the main victim is a woman, as it becomes easy for a person to trap her without any fear.

4. Conditions in rural and urban areas

The conditions of women in both urban and rural area concerning crimes through fake social media accounts is not so good.

Women may have less access to technology and a lower level of digital literacy in rural locations, which might make them more vulnerable to online exploitation and harassment. Because it becomes

[28] *Supra* note 16.

ISSN: 2582-6433

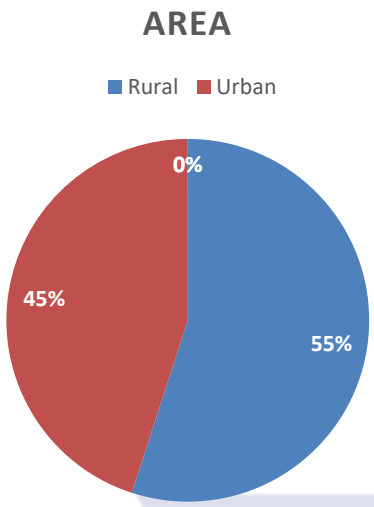
easy for an anonymous person to talk with a girl who didn't have more knowledge about these kinds of instances. Also, the economic disparities in rural areas are a cause of this, because due to it there is a lack of resources and opportunities, and people often use fake social media accounts with malicious intentions to exploit a woman. Rural communities are frequently characterised by close-knit social systems and traditional cultural standards. Girls from such social systems may have less interaction with people outside of their limited circle, so whenever she met with an outsider who seems to be genuine she becomes over-friendly due to which she suffers. The most important reason is that girls in rural areas are not so concerned and aware of their privacy and security while using social media platforms. In those areas, the law enforcement mechanisms are also less. This can discourage the victims from reporting the cases.

On the other side, women are more familiar with social media in urban areas where technology is more accessible. Urban regions often have greater internet access and higher smartphone intelligence rates, more individuals use social media sites. With a growing online population, the probability of meeting fraudulent accounts and online fraud increases. In urban areas communicating and interacting with people is common. Because of the increasing social networking, it may be more vulnerable to befriending and connecting with bogus accounts that look authentic. Trends and social forces can have a big impact on urban areas. Girls in cities may feel obligated to maintain a specific image or online presence, which might make them more helpless to accept friend requests or engage with bogus profiles that match their intended image. Girls may seek affirmation, attention, and social approval through social media sites in the cities. So their situation is bad in being dumped by false accounts that offer approval, admiration, or compliments, making them more subject to manipulation.

Overall, the situation is the same in both the areas urban as well as rural, the factors might be different. But the result is the same i.e. the exploitation of women. Women are becoming victims due to all these factors.

In the research also, the researchers have received almost equal responses from urban and rural areas, which shows the same situation here.

ISSN: 2582-6433



In both areas, 92.9% of women have accounts on various social media platforms, such as 30% having accounts on Facebook, 75.3% having accounts on Instagram, 54.7% having accounts on Snapchat, and so on. 54.7% of these women had faced problems as a result of phoney social media profiles, while 61.2% of them had ignored it. Only 67.1% of women are aware of the legal options available to them, and this understanding is similarly restricted. They just know that they may report accounts, register complaints, and block accounts only.

Therefore, the picture is identical in every area. It shows digital illiteracy is not only the main reason behind this. An educated woman can also be a victim of this. To address this issue promoting online safety education is crucial. Providing individuals with the skills and knowledge to identify fake accounts, and make them understand the privacy settings is needed.

5. Laws governing the issue of fake accounts in India

A fake account is just an account on any social media network where the published information is dishonest, if not fraudulent. Misrepresentation of phoney accounts, as well as the use of fictitious facts, mislead the general public into propagating erroneous information or gathering financial or personal information. The rise in incidences of cybercrime against women in India has prompted constitutional bodies to consider and take harsh action against offenders.

There is no clear rule in place that holds social media platforms responsible for the establishment of

ISSN: 2582-6433

fake accounts inside their network. This is because the network just acts as a middleman and does not directly construct the account.

5.1 Provisions underthe "Information Technology Act of 2000"[29]-

The safe-harbour protection provided by **Section 79**[30] of the Act**,** shields intermediate social media networks from responsibility for third-party information uploaded on their platforms. It states that an online portal that solely accepts, maintains, transmits, or communicates an electronic record is not accountable for any third-party information or communication that is available on it. However, the requirements stipulate that if the intermediary receives 'real knowledge' that any information, data, or communication connection contained in the portal is being used to perform an illegal act, the intermediary is required to remove such content.

There are various other provisions in the **IT Act, of 2000**[31], whitewalls with cybercrimes through fake profiles and by other various means.

- **Punishment for using a communication service to convey offensive messages, etc**. **[Section 66**[32]**]**: This section is triggered when an imposter utilises fraudulent and dishonest profiles to spread spam or viruses or to steal data. The offence is punishable by up to three years in jail, a fine of up to five lakh rupees, or both.
- According to **Section 66C**[33] of the Act, deals with **Identity theft punishment**- "Whoever, fraudulently or dishonestly uses the electronic signature, password, or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to a fine which may extend to rupees one lakh."
- **Sec 66D**[34] of the Act deals with **punishments for personation-based cheating using a computer resource**: "Whoever, using any communication device or computer resource, cheats by personation, shall be punished with imprisonment of either description for a term

[29]*Supra* note 12.
[30] The Information Technology Act, 2000 (Act 21 of 2000), s. 79.
[31]*Supra* note 12.
[32]The Information Technology Act, 2000 (Act 21 of 2000), s. 66.
[33]*Supra* note 13.
[34]*Supra* note 14.

ISSN: 2582-6433

which may extend up to three years, and shall also be liable to a fine which may extend up to one lakh rupees."

- **Section 67**[35](**punishment for electronically posting or transferring pornographic material**)- if the imposter uploads something obscene, vulgar, or appealing to the phoney profile's unhealthy interest, or if the effect is such that it tends to ruin and corrupt those who are likely to read, see, or hear the content contained or embodied in it, given all relevant circumstances. A second or subsequent conviction results in imprisonment of either kind for up to three years and a fine of up to five lakh rupees, and imprisonment of either type for up to five years and a fine of up to 10 lakh rupees.
- **Section 67A**[36]**(a fine or another penalty for the electronic publication or transmission of content containing sexual acts, etc.)**: The Section is activated if the phoney profile includes a sexually explicit act or activity. In the event of a second or subsequent conviction, the punishment is more severe, punishable by imprisonment of either description for a term that may extend to five years and a fine that may extend to ten lakh rupees, and punishable by imprisonment of either description for a term that may extend to seven years and a fine that may extend to ten lakh rupees. The offence is penalised by law, and no bail is available.
- **Section 67B**[37]**(penalties for publishing or sending online content that shows youngsters engaging in sexual acts, etc.)**: If the obscene fake profile is that of a child under the age of 18, the offence is punishable under this section of the Act, which severely penalises child pornography. There is a specific provision for sexual predators that makes it illegal to lure or recruit minors for online interactions for sexually explicit conduct or in a manner that would offend a reasonable adult on a computer resource. The offence is cognizable and non-bailable, and the penalty is similar to that outlined in Section 67A above.
- **Section 69A**[38]which deals with **the ability to order the restriction of public access to any material through any computer resource.** It enables the central government to ask any intermediary to block access or to remove any content or information generated, transmitted, received or stored, or posted by any computer sources.

[35]The Information Technology Act, 2000 (Act 21 of 2000), s. 67.
[36]The Information Technology Act, 2000 (Act 21 of 2000), s. 67A.
[37]The Information Technology Act, 2000 (Act 21 of 2000), s. 67B.
[38] The Information Technology Act, 2000 (Act 21 of 2000), s. 69 A.

ISSN: 2582-6433

"The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021"[39] include several restrictions designed to assist address the annoyance of phoney accounts. According to these standards, every social media site is responsible for establishing a grievance redressal procedure via which complaints can be submitted regarding any content published on that site[40].

As per **Rule 3(2) (b**), if, upon receiving a complaint, the intermediary determines that the impugned content, including artificially morphed images, is similar to impersonation in an electronic form, it must take all reasonable and practicable steps to remove or disable access to such content that it hosts, stores, publishes, or transmits. These guidelines, as well as the grievance redressal process they would develop, would make it simpler for users to report fraudulent profiles. According to the laws, intermediaries must also report cybersecurity issues and share pertinent information with the Indian Computer Emergency Response Team.

5.2Provisions under the"Indian Penal Code, 1860"[41]**-**

These kinds of offences against women are also dealt with in the IPC, 1860[42] in which **Section-416**[43]deals with **cheating by personation**. It states that a person is called to 'cheat via personation,' if he cheats by appearing to be someone else. The impostor would be held responsible whether the individual personated is genuine or fictitious. Anyone who commits forgery of an electronic document for cheating is equally guilty under **Section 468**[44]-"**Forgery for purpose of cheating**".

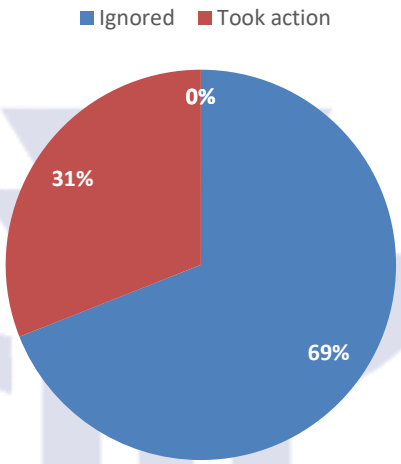
Section 354A[45]- " **Sexual harassment and its punishment**" of the IPC forbids sexual harassment and states that any guy who intentionally distributes pornographic material to a lady against her consent by email, WhatsApp, or any other manner is breaking the law. **Section- 354**[46]deals with cyberstalking which states that any guy who knowingly pursues a woman and approaches her or

[39] Government of India," Information Technology (Intermediary guidelines and Digital Media Ethics Code) Rules, 2021" (Ministry of electronics and information technology, 2021).
[40]India: Legal Action Against Fake Account On Social Media, available at: https://www.mondaq.com/india/social-media/1109666/legal-action-against-fake-account-on-social-media (last visited on May 16, 2023).
[41]*Supra* note 11.
[42]*Supra* note 11.
[43] The Indian Penal Code, 1860 (Act 45 of 1860), s. 416.
[44] The Indian Penal Code, 1860 (Act 45 of 1860), s. 468.
[45] The Indian Penal Code, 1860 (Act 45 of 1860), s. 354 A.
[46] The Indian Penal Code, 1860 (Act 45 of 1860), s. 354 D.

ISSN: 2582-6433

attempts to contact her for personal information despite multiple cautions from that lady will be charged with this offence.

Hence, there are several provisions under the IT Act, of 2000[47] as well as the Indian Penal Code, of 1860[48], but they are of no use if women are not aware of this. The foremost reason behind the increased rate of these crimes is that if any such circumstances appear before any woman she just ignores it and the crime remained unreported and ignored. In this research, 61.2% of women have ignored the situation, as indicated by the Pie chart below mentioned:



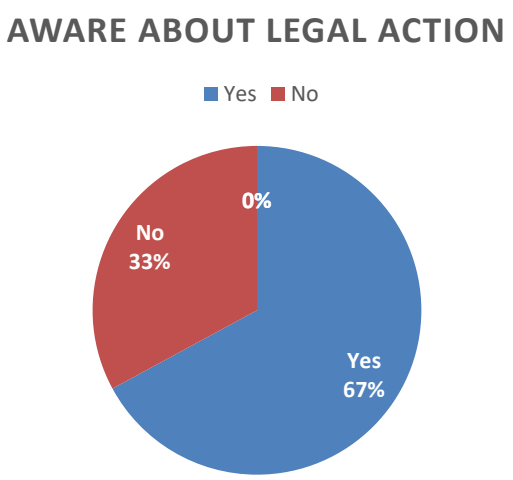
Henceforth, it is very clear that most of the women have ignored these kinds of acts. Only 31% of women have taken some steps and the most common step among them is to report the account. But this is not only the solution.

6. Solutions to tackle crimes through fake accounts

Indian legal system has ample amount of provisions to tackle the problem of crimes through fake media accounts. There are several laws. But the problem is they are not sufficient. Because people are not aware of it. They just know that they can file the complaint but what will be its procedure, what punishments can be given to the accused, what will be its impact on future criminals and so many things they don't know. These are the basic things that every individual should know.

[47] *Supra* note 12.
[48] *Supra* note 11.

ISSN: 2582-6433



There are still 33% of women who are not aware of the legal actions they can take in these situations, as shown by the pie chart. Therefore, lack of awareness is one of the issues which can be resolved by organizing camps, and legal aid programmes by various institutions, and universities in every city and village. So that a large area can be covered. And the victims will become aware that the laws are available for them, for their protection and they can knock on the door of courts for seeking justice. Laws might require social media services to offer users clear and easily accessible reporting tools for reporting false accounts and illegal activity. These processes should be well-publicised and should guarantee that the platform investigates and addresses reported events as soon as possible.

Another major issue is that laws are there for protection but their implementation takes a lot of time. Most of the victims think that they do not want to invite an endless trial so they just simply ignore it. Court proceedings take time but it is well said in Indian Legal System that- **Justice Delayed Is Justice Denied**.

By entering into someone's private information, the accused violates **Article- 21**[49]i.e. the Right to Privacy of the victim. But sometimes the victim is unaware of this right which is his/her Fundamental Right. So again, the issue is a lack of awareness. Every individual must be aware of their basic rights which are Fundamental Rights. Women also have to be more careful while talking with an anonymous person. There are certain privacy policies on social media, they have to read them first and should take necessary precautions.

[49]*Supra* note 16.

ISSN: 2582-6433

It is discussed that there the several laws and Acts to handle these instances but they are not sufficient. The owners of these platforms have to take some serious steps so that the number of fake accounts starts decreasing. They should develop some software which can automatically detect a fake profile and remove it just like Facebook did in year 2022[50]. Apart from this, they can change their requirements for creating a new account and can ask for certain government-issued identification documents. This can help in preventing the creation of fake accounts and make it easier to trace the individuals who are involved in these crimes.

Though the Indian Penal Code contains various provisions for cybercrimes, the issue is that IPC was drafted before digitalization. It contains provisions regarding cybercrime but does not explicitly cover all types of cybercrimes. There should be some addition or amendment in the Act like Sections for emerging offences like cyber threats, hacking, and Identity theft should be included.

Laws can promote and facilitate better coordination among social media platforms, law enforcement agencies, and other relevant players. This can include systems for exchanging information, data, and evidence to help in the identification and punishment of persons engaging in illegal acts via bogus accounts.

The number of persons with specialized knowledge or expertise in cyber forensics should also be increased. The limited availability of these persons hinders the successful investigation.

The liability of the intermediaries is also not defined properly and efficiently, such as internet service providers, and the role of social media in facilitating cybercriminal activities. If their responsibilities and liability are clear, they can ensure their active participation in preventing and addressing these crimes.

Legislation can underline the need for digital literacy, online safety, and awareness efforts to educate users about the hazards of fake accounts, as well as how to identify and report them. This can help individuals, particularly vulnerable groups, become more cautious and vigilant when using social networking platforms.

[50] *Supra* note 9.

ISSN: 2582-6433

Majorly, to keep up with rapidly evolving technology and creative strategies employed by cybercriminals, legislation must be adaptable and flexible. Existing legislation should be examined and revised regularly to ensure its relevance and effectiveness in combating emerging threats.
It should also be noted that legal reforms may not be sufficient on their own. A holistic strategy involving collaboration among stakeholders, including law enforcement authorities, social media firms, educators, and individuals themselves, is vital in combating crimes facilitated by phoney social media accounts.

7. Conclusion

Finally, the prevalence of fraudulent social media profiles is a huge challenge, particularly for girls. Girls, whether from rural or urban areas, are more likely to become victims of various crimes aided by phoney accounts. Examples include online harassment, cyberbullying, identity theft, fraud, and other forms of exploitation. Low computer literacy, economic inequality, social and cultural constraints, the requirement for validation, and the ease with which fake accounts may be formed all contribute to the problem.

Addressing this issue necessitates a diverse approach. It begins with promoting digital literacy and teaching ladies in both rural and urban areas about online safety and privacy safeguards. It is vital to provide females with the knowledge and skills necessary to use social media platforms safely.

Additionally, stricter laws and regulations are necessary to prevent cybercrime using fraudulent accounts. Legislation should prioritise the improvement of identification procedures, the improvement of reporting mechanisms, the clarification of social media platform responsibility, and the expansion of international collaboration. Furthermore, to combat the dynamic nature of this quandary, ongoing regulatory modifications, stakeholder collaboration, and public awareness activities are required.

It is vital to emphasise the protection of girls online, ensuring their safety, privacy, and well-being. By addressing the issue of fraudulent social media accounts effectively, society can work to establish a safer and more inclusive online environment for all girls, encouraging them to use social media platforms confidently and without fear of exploitation.

ISSN: 2582-6433

ANNEXURE I

Draft questionnaire

Fake account victimization: An empirical research, Hi, we are Tanya & Chhavi second-year students of SRM University(Delhi-NCR). We are conducting research which is only for academics purpose, to know more about the prevailing problem of fake social media accounts mostly faced by girls. Your response shall remain confidential. By submitting this form, you acknowledge that your participation is voluntary. Thank you for your valuable time and feedback.

* Indicates a required question

1. Email *

_____

2. Name*

_____

3. Age group?*
   - 16-24
   - 24-34
   - 35-45
   - 45 above

4. Which social media platform you are using?
   - Facebook
   - Instagram
   - Twitter
   - Snapchat
   - Reddit
   - None of the above

5. You are from which area?
   - Urban
   - Rural

ISSN: 2582-6433

6. Do you have an account on any social media platform?
   - Yes
   - No

7. Did you face any problems because of fake social media accounts?
   - Yes
   - No

8. What kind of problem you have faced?
   - Someone is stalking you
   - Someone has used your photos
   - Someone is bullying you
   - Relationship scam by changing religion
   - Any other

9. You took any action against it or ignored it?
   - Took action
   - Ignored

10. What actions you can take against it?

    _____

11. Are you aware of the legal actions that you can take against it?
    - Yes
    - No

12. Is social media safe for girls?
    - Yes
    - No

13. Suggestions on how girls can tackle the issue of fake accounts?

    _____

ISSN: 2582-6433

ANNEXURE II

Sample response sheet: Yashika Saini

Fake account victimization: An empirical research, Hi, we are Tanya & Chhavi second-year students of SRM University (Delhi, NCR). We are conducting research which is only for academics purpose, to know more about the prevailing problem of fake social media accounts mostly faced by girls. Your response shall remain confidential. By submitting this form, you acknowledge that your participation is voluntary. Thank you for your valuable time and feedback.

1. Email *

   Ysforever14@gmail.com

2. Name*

   Yashika Saini

3. Age group?*

✓ 16-24

24-34

35-45

45 above

4. Which social media platform you are using?

Facebook

✓ Instagram

Twitter

Snapchat

Reddit

None of the above

5. You are from which area?

✓ Urban

Rural

ISSN: 2582-6433

6. Do you have an account on any social media platform?

✓ Yes

No

7. Did you face any problems because of fake social media accounts?

✓ Yes

No

8. What kind of problem you have faced?

Someone is stalking you

Someone has used your photos

Someone is bullying you

Relationship scam by changing religion

✓ Any other

9. You took any action against it or ignored it?

Took action

✓ Ignored

10. What actions you can take against it?

Block the contact

11. Are you aware of the legal actions that you can take against it?

Yes

✓ No

12. Is social media safe for girls?

✓ Yes

No

13. Suggestions on how girls can tackle the issue of fake accounts?

It is important to keep information about the fake profile by taking screenshots or printing out the profile pages. This may be useful if the issue continues and you need to work with the platform or the police to resolve the issue.