



INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

IJLAR

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

IJAR

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

IJLAR

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

IJLAR

DIGITAL GENDER DIVIDE AND CYBERCRIMES **AGAINST WOMEN**

AUTHORED BY - S. SRINITHI & S. SEETHA LAKSHMI

INTRODUCTION

These days we can see rapid expansion in digital technologies. It has transformed the traditional society into a contemporary society, reshaping the way individuals do an act. With the development of technology, communication, money transaction, access to information, and participation in governance have changed. In India, the awareness and programs for digital technology and the rise of internet facilities have been major factors towards the change of the digital environment. We can see that these have contributed towards various opportunities in various sectors like education, economic growth and entrepreneurship. But these opportunities are not available equally in all societies. Still, some of the rural areas do not have proper facilities and awareness for digital technologies. Specifically, women in rural societies are facing significant barriers in using the internet facilities safely. This is called the digital gender divide. According to reports from various sources, some of the main reasons women face digital gender divide are

1. Patriarchal social norms and gender stereotypes
2. Economic inequality
3. Lower education and digital literacy levels
4. Rural-urban disparities
5. Household responsibilities and time constraints
6. Safety and security reasons
7. Limited decision-making power
8. Language and accessibility barriers
9. Underrepresentation in technological fields
10. Inadequate awareness and policy implementation

The increased use of digital technologies in everyday life have increased the exposure of women to be victims of cybercrime.

India has seen a significant rise in cybercrime against women. According to reports of 2026, offences such as cyberbullying, cyberstalking, identity theft, identification theft, sextortion, pornography and AI deepfake pornography have risen as dangerous threats to women's dignity. These crimes increase the amount of fear, psychological trauma, financial loss, and social isolation among the victims. Many women face discouragement due to fear of victim-blaming, low confidence in law, and lack of awareness, which allows the criminals to exploit the stakeholders. The existing scholarship primarily addresses the digital gender divide as a developmental challenge affecting education, employment, and economic participation while, cybercrimes are predominantly analyzed through the lenses of criminal law, cybersecurity and technological regulation. This gap has demanded a more integrated approach which analyses the overlap between digital inequality and cybersecurity.

This paper argues that digital exclusion functions as a main factor for cyber victimization. It also argues that it should no longer be viewed merely as a question of technological access or social development. The paper proposes a conceptual framework showing a development from “digital exclusion to digital illiteracy, reduced cyber awareness, increased vulnerability, and ultimately cyber victimization”, thereby establishing the direct relationship between the digital gender divide and cybercrimes against women. It also analyzes the difficulties posed by artificial intelligence, especially the deepfake technology and AI-enabled gender-biased cyber violence. It also suggests some suggestions to reduce the cyber vulnerability. This paper seeks to contribute a novel perspective on protecting women in this digital society.

UNDERSTANDING THE DIGITAL GENDER DIVIDE:

It means inequality in access to, use of, and participation in digital technology. Despite the government's efforts to close this gap, persistent challenges like patriarchal norms, safety concerns, affordability issues, and limited access in education make it a strenuous job for the government. Addressing the digital gender divide is considered to be essential for achieving broader gender equality, inclusive economic development and equitable digital transformation. Let's see the causes of the digital gender divide in India. ¹

¹ <https://www.ideasforindia.in/topics/social-identity/digital-gender-divide-amidst-india-s-service-led-growth>

1. **Patriarchal Social Norms:** This is the foremost reason for many deprivations. Deeply rooted patriarchal social norms prioritize men over women. So, women in this kind of family will not have much access and exposure to the digital environment.
2. **Economic constrain:** This is a common problem for both men and women. But, considering the social culture of India, employment opportunity, salary and standard of living makes it even more difficult for women. Many women in the unorganised sector are still not getting the payment for the work that is being done by them. So, they are not able to afford a smartphone. Even if they can buy a smartphone, a monthly consistent recharge could be challenging.
3. **Educational disparity and digital illiteracy:** Still today many girl children in villages are not getting proper education. And even if they own a smartphone and have an internet connection, they are not digitally literate, which means they do not know the perks of the internet, do not know how to safely use social media, and have difficulty in handling digital transaction.
4. **Limited access to digital infrastructure:** Poor connectivity issues, unreliable electricity and limited availability to digital services is a main reason that increase the gap.
5. **Safety concerns:** Many women are not using the internet and online communities out of fear. Online crimes, as we already discussed, like cyberbullying, online grooming, online stalking, threats, etc. are discouraging women from participating in the digital world.
6. **Inadequate gender inclusive policies in India:** This is one of the major setbacks. The Government has introduced many schemes and policies like Digital India, Pradhan Mantri Gramin Digital Saksharta Abhiyan, National Educational policies, etc. All these policies are not serving their objective because of implementation issues. Poor implementation of policies, not covering the entire intended objective and community, makes it even more difficult to fill the gap and rectify the problem.

CYBERCRIME AGAINST WOMEN:

The rapid growth of social media has exacerbated cybercrimes against women by making it easier for the offender by providing easy access. In general, the crime rate happening against women is higher than that against men, but it is increasing day by day. According to the report of the committee on the empowerment of women on “Cybercrimes and Cyber Safety of women” on 23rd

March 2026, there is a rise in cybercrimes targeting women and children including cyberstalking, sextortion, Nonconsensual dissemination of explicit sexual information, online grooming, deepfakes and online harassment. As per the National Crime Report Bureau it has been noted that between 2017 and 2022 there has been a 239% increase in cybercrime against women and children in India. Now, it has raised as an imperative concern that needs an efficacious preventive measure. Let's see the various types of cybercrimes against women²:

1. **Sharing explicit content without consent-** This has become a common problem nowadays. Many people are using this as a tool to blackmail. This is not only infringing on the privacy of the victim but also gives psychological pressure.
2. **Hate speech-** Also a common form. Many people are misusing their right to speech. Without any boundaries, thinking that they have every right to say whatever they want, even talking ill about other people, has now become a common problem. This happens frequently when a woman influencer posts anything on social media. Sometimes this goes to the extent of suicide.
3. **Threats and abusive message-** Women often face the threat of physical harm and abusive messages and hate speech, which can escalate to real world threat.
4. **Blackmailing and Extortion using explicit content-** Preparators often use explicit content for blackmailing for money and extortion.
5. **Phishing scams-** This is not something that is happening against women only. They are being affected by this largely.
6. **Online grooming-** This is one of the escalating worries. Especially children between the ages of 16 to 18, teenage and early adults, are targeted and trapped. In this type the predators will be emotionally connected with the victim, and they make the victim believe that they are the safest person to trust. They will be using the trauma of the victim or any other mental stress to build that connection. And once they are well connected, they will manipulate the victim for sexual exploitation or traffic them.
7. **Doxxing-** Intentionally releasing all the private and personally identifiable information of an individual without their consent. This is often used when the victim is not complying with the directions of the predator.

² <https://blog.ipleaders.in/everything-about-cybercrimes-against-women/>

8. **Sextortion-** Blackmailing with the victim's sexual image or any information. This is used for ransom or for any other sexual favors.
9. **Revenge pornography-** This is similar to doxxing. Here the predator will be connected to the victim. Victim's ex-partner or acquaintance or harasser or stalker will be using victims' nude pictures to intimidate them.
10. **Cyberstalking-** This is also a common issue. Where the predator will be constantly monitoring the victim's social media profile or any accounts of the victim to seek revenge or to instil fear or emotional and mental distress.

These cybercrimes will cause serious mental distress, emotional trauma, financial setbacks, long-term identity issues and a pervasive loss of trust in the digital environment. These types are not exhaustive.

THE MISSING LINK: HOW THE DIGITAL DIVIDE INCREASES CYBER VULNERABILITY

The increasing number of cybercrimes against women cannot be understood by analyzing only the limitations of law and technological advancements. One of the main factors that is not being looked upon is the digital gender divide, resulting in structural inequalities that increase cybercrime against women. It is not only an issue of unequal access to technology. It also includes digital illiteracy, lack of cyber awareness and lack of confidence. These lags will make women more prone to cyber vulnerability. This paper explains how the digital gender divide increases cyber vulnerability through the following framework:

Digital Gender Divide -> Limited digital Literacy -> Reduced Cyber Awareness -> Weak Digital Safety Practices -> Increased Cyber Vulnerability -> Cyber Victimization

This framework explains to us that, there is a chain of incidents that leads to Cyber-Victimization.

1. **Digital Gender Divide:** This refers to the lack of equal access to technologies and technological opportunities for women due to the social norms, economic dependence, educational disparities and the rural-urban differences. This reduces the participation of women in the digital sector. So, they are behind in time to explore the digital technologies compared to men.

- 2. Limited Digital Literacy:** The digital gender divide leads to limited digital literacy. Women will lack skills that are required to access the technologies safely. They lack familiarity in identifying fraudulent websites, using two-factor verification or understanding the privacy settings. When a person accesses the technology without proper knowledge, they easily become a victim of cybercrime.
- 3. Reduced cyber awareness:** The limited digital literacy leads to reduced cyber awareness. Women may not know the warning signs that are given when they are exposed to cyberstalking, online impersonation, financial fraud or AI-generated deepfakes. They may also lack the awareness of reporting mechanisms through cyber portals or keeping the evidence safe for further procedures while reporting a cybercrime. Due to this reason, the cyber officials cannot investigate properly, and thus complaints go unreported. Not only these technological lags make the women to not report the cybercrime against them. Social factors such as victim-blaming and lack of family support also restrain the women from reporting.
- 4. Weak Digital Safety Practices:** The lack of awareness leads to unsafe practices. The cybercriminals use this lack of awareness and steal the personal information through hacking. The cybercriminals also use the photos of women to morph and earn money through that by blackmailing them that they will post it in the online platforms. Not only photos, but they also make fake videos through AI and publish them on the porn sites. When they do not report the cybercrime, the criminals do not fear and use this an opportunity to involve in more such crimes.
- 5. Increased cyber vulnerability:** All the above-mentioned factors increase the cyber vulnerability. This makes the women excluded and disproportionately exposed to cybercrimes. The new AI technologies have further increased the risk of cyber vulnerability. Through AI, the criminals make deepfake pornography, voice cloning, etc.
- 6. Cyber Victimization:** This framework shows us that cyber victimization is not caused only because of criminal behavior but also concentrates on the factors of technology. So, to reduce cyber victimization, it not only requires addressing cybercrimes but also requires more than stronger criminal laws. The government should provide proper cyber policies or create separate legislation for cyber laws. The already existing laws are not protective, and

there is no proper separate legislation. The government must also spread awareness among the women in cyber technologies.

LEGAL FRAMEWORK AND ITS LIMITATIONS

India has established legal frameworks that recognize cybercrime against women, like the Information Technologies Act, 2000 and the Bharatiya Nyaya Sanhita, 2023. These acts merely punish a person who committed the crime but does not have any preventive measures to avoid the crime. They do not recognize the role of the digital gender divide.

Article 14 of the Indian Constitution provides equality before law, i.e every person is equal in the eyes of the law.³ Article 15 prohibits any form of discrimination based on gender⁴. Article 21 gives protection for a person's personal liberty. Even though these provisions exist, the practical problem still exists. These provisions are in a broader perspective while it requires effective implementation against technology-enabled offences.

Section 44 of the Information Technology Act, 2000, punishes unauthorized access and damage to computer systems. Section 66 C punishes identity theft, digital signatures, and fraudulent use of passwords and other electronic identifiers. Section 66 D criminalizes cheating by impersonation through computers. Section 67 punishes the publishing and transfer of any obscene material. Section 67 A provided strict punishments for the offence, which involves publication or transmission of sexually explicit content.

Section 77 of BNS punishes sharing intimate images or videos without consent. Section 78 punishes stalking online. Section 79 criminalizes sending abusive or obscene messages to women through electronic communication. Section 296 punishes publishing obscene acts and songs. Section 319 punishes cheating by personation.

Limitations

- 1. Reactive rather than preventive:** Despite these legal protections, the cybercrime against women is increasing. These legislations are “reactive rather than preventive.” These legislations give punishments but do not prevent these cybercrimes. They do not contain

³ Article 14 of Indian Constitution

⁴ Article 15 of Indian Constitution

provisions for digital literacy, cyber awareness or preventive education. Women who lack awareness of the digital technologies are prone to become cybercrime victims despite the existing legal frameworks.

2. **Low awareness of legal remedies:** The lack of awareness reduces the effectiveness of these existing legislations. Many victims are unaware of the cybercrime reporting portals or the procedures to file a complaint against the criminal. They do not save the evidence, which will be required during the procedure. Without proper evidence, the investigation becomes unsuccessful and becomes difficult to find the criminal.
3. **Emerging Technologies:** The existing legal frameworks find it difficult to keep up with the emerging technologies. There is an absence of specific statutory recognition, which creates uncertainty.
4. **Practical challenges:** There are practical difficulties like jurisdictional issues, inadequate digital forensic infrastructure and delays in prosecution. Social barriers like fear of victim-blaming, reputation, and lack of support from family restrain the victims from filing a complaint.

This analysis shows us that, despite the existence of current legal frameworks, there are limitations. They only punish the criminals but do not have any provision to prevent the cybercrime. The main lag is the lack of provisions for the digital gender divide, which is mainly discussed in this paper. Laws alone cannot reduce the cybercrimes. There should be proper policies that promote awareness against cybercrimes, digital inclusion of women, etc. To bring an effective response, there should be a separate legislation having punishments for the cybercrimes, including the emerging technologies combined with the provisions that ensure women's right to participate safely in the digital environment. The legal framework must integrate these two things to effectively prevent the cybercrimes.

EMERGING THREATS

This is a new pattern of crime. Where attackers are using AI to boost their outreach and automation like automated and convincing messages, use it to experiment with many methods to commit crime. AI has been used in two ways: attackers using it like this. But defenders using it detect suspicious activities and respond to threats even faster than human.

1. **AI-Boosted Phishing and Business Blackmails-** The victim's voice, language, tone and handwriting are being used by criminals to write a well-structured message exactly like the victim's language and tone to blackmail and manipulate them. They can easily rewrite the same message to make it suitable for their job.
2. **Deepfake enabled impersonation-** Synthetic video and audio of the victim used for "urgent payment" scams, impersonated approvals, fraudulent outreach. Even imperfect impersonation will also work when the victim is in a rush, or when the victim is speaking in a noisy place.
3. **AI Accelerated Malware and script Generation-** Instead of writing every code line by line manually, now cybercriminals can easily use AI to write a whole code within a short time and generate "living-off-the-land" scripts, which will use the legitimate tools already present on the victim's device and use them for malicious activity. Generally, trusted system tools find it difficult to detect the attack.
4. **Credential and session theft-** AI makes it easy for the cybercriminals to steal passwords and login information from users at a larger scale. AI can automate these attacks by selecting targets and adjusting timing to avoid detection, and the attacker can learn from their failure to avoid mistakes in the subsequent times.
5. **Scam Content Factories-** AI allows scammers to produce false and fraudulent content and information at a larger scale. What once required a whole design and team now can be made within a short time. Fake banking or shopping websites, counterfeit apps and AI-powered customer chatbots are example of this.⁵

This is not an exhaustive list of crimes. The list may go long.

RECOMMENDATIONS

The increasing rate of cyber crimes against women shows us that there are no proper policies to protect the women and to prevent the cybercrime. Since the digital gender divide majorly contributes to women's cyber vulnerability, there should be effective policies and the government must promote cyber awareness and digital inclusion.

⁵ <https://socprime.com/blog/siem-edr/what-are-the-main-ai-assisted-cyber-attacks/>

- 1. Legal Measures:** The legal framework must be updated with the latest digital technologies. Government must consider introducing separate legislation for cybercrimes which includes the digital gender divide and such other cybercrimes. There must be specialized cyber units with trained digital forensics to ensure faster investigation. This ensures timely justice.
- 2. Educational Measures:** To bridge the gap in the digital gender divide, there should be sufficient investment in digital literacy. Governments, educational institutions and NGOs must spread awareness among the women and children in the rural areas. This awareness must not only be about digital access; it should also speak about different cybercrimes that exist in society and also explain the legal remedies if they become a victim of cybercrime.
- 3. Institutional Measures:** There should be an effective cybercrime cell to report the complaints against the cybercrimes. It should provide programs that increase awareness among the stakeholders. There should be a National Cyber Crime Reporting Portal and helplines set up by the Central Government. There should be grievance redressal and psychological counselling for the victims of the cybercrime. Government should collaborate with institutions to provide effective mechanisms.
- 4. Technological Measures:** Technology companies must adopt strong safety measures to protect women from becoming a victim of cybercrime. Social Media platforms must adopt advanced safety measures to reduce deepfake content, image morphing and content that affect the dignity of women. Default privacy settings should be adopted.

The ultimate goal of the government should be preventing the cybercrime and not punishing the cyber criminals. It should shift from a punitive method to a preventive approach. Digital inclusion should be the essential factor of cyber security and women's empowerment in contemporary India.

CONCLUSION:

A rapid growth of digital infrastructure in India has created an unprecedented growth in opportunities, easy access to education, social and economic inclusion. But the digital gender divide and cybercrimes against women pose a serious problem that needs to be addressed. Economic conditions, family background, literacy and availability of digital sources are major setbacks for the inclusion of women into the digital environment. Even those who have access to digital sources are afraid of safety issues. So, this paper highlights all these problems and suggests

some recommendations that will be useful for addressing and redressing the problems. Inclusiveness means including all kinds of people in every activity. So, include every woman in the digital environment with a policy that should not only monitor but also prevent cybercrimes and encourage women to access it freely.

