

Click, Share, Harm: Social Media's Role in Violating Privacy of Domestic Violence Victims in India

Isha Kansal¹, Dr. Ankur Sharma²

¹RESEARCH SCHOLAR, SCHOOL OF LAW, GD GOENKA UNIVERSITY, SOHNA, HARYANA
CONTACT NUMBER- 9770994452
E-MAIL ID- kansalisha5@gmail.com

²ASSISTANT PROFESSOR, SCHOOL OF LAW, GD GOENKA UNIVERSITY, SOHNA, HARYANA
CONTACT NUMBER- 9828210786
E-MAIL ID- advocateankur21@gmail.com

ABSTRACT

In the digital age, social media is both a source of empowerment and exploitation. It is a significant risk to the privacy of domestic violence survivors in India as it involves unauthorized disclosure of identity, cyberstalking, online harassment, and doxxing. Despite constitutional safeguards under Article 21 (Right to Privacy) and legal provisions such as Protection of Women from Domestic Violence Act, 2005, Digital Personal Data Protection Act 2023 and Information Technology Act, 2000, there are critical gaps that exist in protecting survivor privacy in the digital space. Social media platforms not only fail to effectively moderate content but also do not implement survivor-specific privacy settings and robust reporting mechanisms for safeguarding victims from further victimization. This article discusses the legal, social, and technological challenges related to the violation of privacy of domestic violence victims on social media in India. It also looks at international best practices, such as confidential address programs and stronger anti-doxxing laws, to suggest policy reforms and digital safety measures that can ensure better protection for survivors. Hence, the study emphasizes legal amendments, strict enforcement of cyber laws, and accountability for social media sites in order to provide a safer and better digital environment for survivors of domestic violence.

KEYWORDS: Domestic violence, privacy violation, social media, cyberstalking, right to privacy, online harassment, legal framework, India

INTRODUCTION

In the age of digital connectivity, social media platforms have become an essential tool for communication, socialization, and information dissemination. Increasingly, these platforms are also used to raise awareness about societal issues, including domestic violence. However, for many survivors of domestic violence, social media has emerged as a double-edged sword. While it could provide a platform for victims to narrate their stories, reach out for support, and seek justice, it exposes them to harsh privacy violations like unauthorized disclosure of personal details, cyberstalking, and harassment. In India, the growth of social media has been tremendous, and this has exposed more and more victims of domestic violence to further victimization. This problem of privacy invasion on social media is much more worrisome because the survivors typically suffer an amplification of their traumatic experience and are exposed to public judgment, online threats, and even physical attacks.

Privacy, as it is understood, is a right protected by the Indian Constitution under Article 21 guaranteeing the right to life and personal liberty. Puttaswamy v. Union of India, recognized the right to privacy as a fundamental right, highlighting its significance in safeguarding personal data and dignity. Despite this constitutional safeguard, privacy protection for domestic violence survivors in the digital world remains inadequate. The Protection of Women from Domestic Violence Act (PWDVA), enacted in 2005, offers critical legal protection for women suffering from domestic abuse. This law does not, however, provide specific solutions for the needs of digital privacy among survivors, who remain at risk for online harassment and exposure of identity. Likewise, the Information Technology Act, 2000, dealing with cybercrime, has some

remedies against online harassment; however, the remedies are generally not enough in domestic violence cases wherein perpetrators use social media to intimidate and control victims further.

Social media are well-constructed communication tools, but they also become an opportunity for abusers to access their victims in ways never known before. For instance, perpetrators of domestic violence often leverage those platforms to track the survivor, alter stories, and humiliate them in public. The violence transcends the physical and psychological realms into that of the digital world: experiences most intimate and sacred to survivors are posted without their permission; their identities and personas are launched into the public arena; and privacy is usurped. The consequences of such an exposure are far-reaching, often ending in re-victimization, emotional distress, and even physical danger. For instance, in a public sharing of their story on social media platforms to garner support or seek justice, survivors become exposed to harassment, threats, and retaliation by their abusers. In addition, the fact that most social media platforms have no privacy settings allows perpetrators easy tracking of the activities and location of survivors.

The most alarming concern is the issue of doxxing, which refers to making public private information. Abusers can post private details such as home addresses, phone numbers, or sensitive personal history, which online mobs or other perpetrators use to harass and harm survivors. With the rising numbers of laws against online harassment and taking particular matters for protecting privacy, legal protection gaps leave many survivors vulnerable to digital abuse. For example, Section 66E of the Information Technology Act, 2000, criminalizes the dissemination of private images without consent, but this provision is rarely invoked in cases of domestic violence, where the abuse is often more subtle and insidious. In addition, most social media platforms have been criticized for not acting immediately against harmful content and instead tend to prioritize freedom of expression over the protection of vulnerable individuals.

Legal protection in India has been unable to keep pace with the rapid pace of technological development, leaving wide gaps that abusers can exploit. Cybercrime laws provide some level of protection, but there is a lack of nuanced understanding of the unique risks that survivors of domestic violence face online. In this regard, the Indian legal system has not yet recognized the full extent of online privacy violations and the cyber-related risks that victims face. Internationally, such countries as the United States have introduced confidential address programs. There, survivors of domestic violence are allowed to maintain their addresses in secret from the abusers. Other countries, like the United Kingdom, have explicit legal protections for online privacy. In fact, such countries criminalize the exposure of victim identities and impose penalties on digital abuse. Such measures require the implementation of deeper reforms in India to strengthen the legal framework for protecting digital privacy of domestic violence survivors.

This article explores the role of social media in violating privacy against domestic violence victims in India by analyzing the legal gaps, technical vulnerabilities, and the social implications of their violated privacy. The role of social media in facilitating digital abuse will be highlighted and ways to strengthen privacy protections for survivors through policy will be proposed. In addition, it will identify how India's legal framework can evolve to address the rising challenges posed by this digital age, thereby ensuring survivors do not get harmed further in the online world.

PRIVACY VIOLATIONS OF DOMESTIC VIOLENCE SURVIVORS ON SOCIAL MEDIA

Social media tools provide a tremendous means of interacting, sharing, and seeking help among people living in today's highly interconnected world. However, for survivors of domestic violence, social media also presents an easy route to increased abuse, exacerbation of trauma, and vulnerability to privacy violations. Four key privacy violations on social media experienced by survivors of domestic violence will be discussed. These include, but are not limited to: unauthorized exposure of survivor identities; cyberstalking and digital harassment by abusers; doxxing and online vigilantism; and the failure to take steps toward digital safety for victims. Each of these is a particular challenge in defending the rights and dignity of survivors in the digital age.

1. Unauthorized Exposure of Survivor Identities

One of the most serious privacy violations that survivors of domestic violence face on social media is the unauthorized exposure of their identities. Survivors often seek refuge by sharing their experiences online, either to find support, raise awareness, or seek legal remedies. However, their attempts to use social media platforms for empowerment can backfire when their personal details, including names, photos, and addresses, are shared without their consent.

This can be both intentional and unintentional. Sometimes, the media or social media users post information about the survivors of domestic violence to sensationalize their stories or to show how severe the abuse was. For example, when a survivor decides to make a police report or seek legal protection in a court of law, the facts about their case and even their identity may be exposed online by the media or in the form of social media posts. This unintended release can have the most severe impacts because survivors usually fear retaliation from their abusers and societal judgment.

Moreover, discussing private aspects of a survivor's life without any form of approval from them becomes an avenue leading to secondary victimization, that is, the judgement or blame coming from the people in the street or online sites about the survivor's status. This ends up isolating the survivor again and discouraging other victims seeking the same remedies. This issue calls on privacy protection in the digital space and the right to anonymity, especially by survivors who have already experienced considerable trauma.

2. Cyberstalking and Digital Harassment by Abusers

Cyberstalking and digital harassment are some of the most common and insidious forms of online abuse experienced by domestic violence survivors. Abusers often exploit social media platforms to maintain control over their victims, even after they have physically escaped the abusive relationship. Stalking has traditionally been understood as a form of offline behavior, but in the digital era, it has evolved into a pervasive online activity.

Abusers can use social media platforms, including Facebook, Instagram, and Twitter, to track the victim's online activities, monitor their whereabouts through location-tagging, and send threatening or harassing messages. They may also create fake profiles to impersonate the survivor, manipulate the survivor's online presence, or threaten them with exposure. This kind of harassment is most disabling because it attacks a survivor's feeling of being in control or able to maintain her safety, which often seems to entail feelings of being trapped that can have long-term psychological implications.

Revenge porn or non-consensual distribution of private images is an example. Survivors may have shared private images with their abusers at one point, but those images were later used on social media as a form of retaliation or to further control. The emotional distress of this form of digital abuse is profound because survivors feel publicly humiliated, threatened, and further isolated from their communities. In most scenarios, the law has provided limited redress for such occurrences, making its victims feel helpless.

3. Doxxing and Online Vigilantism

Doxxing is another very harmful kind of privacy violation that survivors of domestic violence experience via social media; publicizing private information about a person without his or her consent. It's particularly damaging with survivors of domestic violence because the practice can be used to hurt them physically, threaten them, and continue hounding them. Doxxing often involves providing personal details about a survivor - home address, phone number, or place of work - and this makes it easier for an abuser, or even someone who is unknown, to trace and intimidate him or her.

Abusers may use doxxing to retain control over the victim, especially if the survivor has escaped the abusive relationship or filed a legal case. This is because, by leaking personal information, the abuser ensures that the survivor lives in a state of fear of being found or physically assaulted. In some cases, online vigilantes also engage in doxxing, claiming to expose the abuser's actions to the public, without considering the harm it does

to the survivor. These vigilante actions can dehumanize the victim, further contributing to their victimization by forcing them into the public eye.

In many ways, this can be compared to the so-called online justice that some individuals argue doxxing is, because it often takes away a survivor's ability to control the narrative and exercise their right to privacy, particularly when they don't want attention or revenge. Furthermore, without proper regulation in place on social media platforms, the act of doxxing frequently goes unpunished, leaving the survivors few options for remedy.

4. Lack of Digital Safety Measures for Victims

Online abuse has become prevalent; however, social media services have lagged behind in implementing real remedies for the privacy and safety of victims. Facebook and Instagram have added blocking and reporting features, but these have proven inadequate to stop stalking or harassment from becoming worse.

In many cases, the survivor's complaints are ignored or delayed by the platform moderators, who are usually overwhelmed by the number of reports. This lack of timely response leaves the survivor further isolated and unprotected from harassment. Furthermore, privacy settings are usually complicated and hard to navigate, especially for people who are not tech-savvy or familiar with the intricacies of digital security.

One of the strongest obstacles in the way of effective privacy protection is the lack of survivor-specific safeguards. Platforms do not offer automatic privacy settings or specific protocols for those going through digital abuse stemming from domestic violence. Therefore, these survivors end up taking things into their own hands, monitoring their social media presence and manipulating settings all the time, which eventually wears out and beats them both physically as well as emotionally.

LEGAL PROTECTIONS AND GAPS IN INDIA

The legal framework pertaining to the right to privacy for survivors of domestic violence in India, especially in cyberspace, has undergone a development process over time. Although the laws are adequate to some extent, there exists a significant loophole in the proper enforcement and implementation of these laws, especially pertaining to the specific vulnerabilities a survivor faces through social media or other digital forms. This section discusses the central legal provisions existing for privacy protection in the area of domestic violence and the lapses in the Indian legal scheme.

1. Privacy Rights under the Constitution

While the Indian Constitution is silent on this right, it has emerged as a core right under Article 21 that contains the right to life and liberty. In this regard, this section deals with the case law of *K.S. Puttaswamy v. Union of India*: The Supreme Court of India declared that the right to privacy is a fundamental right that protects the dignity, autonomy, and personal freedom of an individual. This judgment has deep implications for privacy protection, especially in cases of domestic violence where a victim's personal information, including identity, location, and experiences, can be exposed without consent.

Although this right is recognized, it is not absolute, and reasonable restrictions can be imposed, especially on matters of national security and public order. In the context of domestic violence and privacy violations, however, this right remains crucial because it ensures that survivors are entitled to confidentiality regarding their personal and intimate details, especially when they seek legal recourse or support.

2. Protection of Women from Domestic Violence Act (PWDVA), 2005

The Protection of Women from Domestic Violence Act, 2005, is a landmark legislation that protects women from domestic abuse, including physical, emotional, and economic violence. The Act provides comprehensive protection by recognizing various forms of violence, including emotional, psychological, and sexual abuse, and offers remedies such as protection orders, residence orders, and monetary relief.

However, the PWDVA is silent on some of the most glaring digital vulnerabilities that survivors experience—for example, online harassment or the unauthorized public disclosure of personal information via social media. For instance, if a perpetrator publicizes intimate pictures or private details of a survivor over the internet, the Act is silent on those violations specifically and does not address legal remedies under the digital framework. Though the law promises relief in respect of physical violence and economic abuse, there are no provisions under it which may safeguard survivors from cyberstalking or any other kind of digital abuse leading to further victimization and revictimization.

3. Information Technology (IT) Act, 2000

The IT Act, 2000, is the most dominant legislation that is specifically based on India in order to combat the cybercrime issues and offenses arising in digital modes. Specifically, Section 66E of the IT Act criminalizes the dissemination of private images without consent, providing a means for survivors to seek legal remedy in cases of revenge porn or unauthorized distribution of personal content. This provision is vital for addressing some forms of digital abuse, such as when abusers share intimate images or videos of survivors on social media to exert control or threaten them.

Besides, Section 354C of the IPC under the IT Act deals with voyeurism and cyberstalking. Criminal remedies are available in cases where the perpetrator secretly records or shares intimate content of the survivor. Despite these provisions, the IT Act does not adequately address the broader issue of online harassment or doxxing (the public release of personal information), which are significant concerns for survivors of domestic violence in the digital era. Moreover, the enforcement of these provisions remains inconsistent, and victims often struggle with slow legal processes and complex procedures for addressing online abuse.

4. Digital Personal Data Protection Act, 2023

Digital Personal Data Protection Act, 2023 is the newest piece of legislation to find its way in the country's lawbook. This new piece of legislation will further look after safeguarding an individual's personal data. It underlines the significance of safeguarding one's personal data, while in collection, processing, or even storing through such entities as is operational within the territory of India. One of its significant provisions is that companies must obtain explicit consent from individuals before collecting their personal information, thereby ensuring that survivors of domestic violence maintain control over their data.

The Digital Personal Data Protection Act does not fully address the nuances of digital abuse in the context of domestic violence, even though it provides a robust framework for data protection. While being more concerned about corporate data practice and not with such specific vulnerabilities confronted by the victim of domestic violence, doxxing, cyberstalking, or publication without his/her permission of private/intimate images/photographs/ recordings, etc, online privacy violation in domestic violence case finds inadequate protection with the current provision of this Act.

5. Gaps in Indian Legal Framework

Despite the progress that such laws have taken, several voids in the legal system of India prevail. First, laws regarding cybercrimes in India remain fragmented and disorganized; varied definitions of online abuse and privacy violation create confusion and hinder the law implementation process. Some forms of online abuse, such as sending messages or threatening communication, are dealt with by the IT Act. It does not embrace the complete horizon of digital offense that the victims of domestic violence may face.

Additionally, ignorance by the public and legal professionals on the exact nature of digital abuse makes cyberstalking and doxxing not to be included as part of domestic violence. Victims are confused on whom to seek help from when their abuser is targeting them online, and most social media platforms fail to implement reporting mechanisms that take care of the survivor's safety.

The lack of specialized protections for digital data in cases of domestic violence survivors clearly leaves no well-defined legal mechanism for such protections. The laws regarding online harassment, doxxing, and

revenge porn have been inconsistent and hard to enforce, thus leaving several survivors without remedies. The power of social media platforms, which facilitate abuse, rests considerably in self-regulation by social media companies, whose policies may not always be aligned with the law or the needs of victims.

SOCIAL MEDIA COMPANIES AND THEIR ROLE IN PRIVACY VIOLATIONS

Social media has become an important source of support, sharing experiences, and resource access for survivors of domestic violence. However, social media also presents a significant privacy risk because poor policies and lack of enforcement mechanisms often expose survivors to re-victimization, harassment, and digital abuse. The social media companies are in charge of ensuring that privacy and safety concerns for users, such as those that affect the most vulnerable among them- domestic violence survivors, are respected. Yet again, the firms are usually inefficient in two respects: they are incapable of concealing the survivor identities and report response mechanisms inadequately.

1. Failure to Protect Survivor Identities

One of the most significant manners in which companies operating social media contribute to privacy violations involves failing to provide adequate protection to the identities of domestic violence survivors. Many platforms allow for users to customize their privacy settings, but it is often unclear, hard to find, or insufficient to truly prevent unwanted exposure. Survivors may try to remain anonymous and limit access to their personal information; however, by default public settings or data-sharing policies often leave the survivor vulnerable to unwanted exposure.

Social media sites often collect and track user data, sharing it with third-party advertisers and data brokers. Such data includes location history, personal connections, and browsing behavior, which can be used by abusers or online harassers to track survivors. In some cases, facial recognition technology and auto-tagging features have inadvertently exposed survivors who were trying to remain anonymous.

In addition, algorithmic suggestions may present a serious threat to survivors. For example, platforms such as Facebook and Instagram will suggest friends based on past interactions. Survivors may thus be exposed to their abusers or individuals connected to them. Survivors who open new accounts in order to evade their abusers are still suggested as friends to their old networks, thus making it easier for the abuser to trace them. This is a failure of social media companies to understand the particular risks facing survivors of domestic violence, hence showing lack of privacy-sensitive design.

2. Inadequate Reporting and Response Systems

The other major failure of social media companies is having an ineffective and delayed response to privacy violations, harassment, and digital abuse. Platforms have mostly installed reporting mechanisms for harassment, doxxing, and revenge porn, but these systems turn out to be slow, inconsistent, and non-transparent. Survivors who report their violations on privacy experience long delays before any action might be taken.

Many victims of domestic violence suffer from cyberstalking, non-consensual image sharing, and online threats. Social media networks often fail to remove harmful content or ban abusive accounts in a timely manner. In cases of doxxing—where a survivor's personal details, such as their address or phone number, are publicly exposed—swift removal of the information is critical to prevent physical harm. However, platforms often fail to act quickly, leaving survivors vulnerable to harassment, threats, and potential real-world danger. Moreover, the social media companies often fail to recognize context-specific abuse through automated moderation tools, which results in harmful content remaining online even after being reported. Survivors often have to report the same violations multiple times before any action is taken, thereby increasing their distress. Many platforms often opt for freedom of speech over survivor protection, where the abusers can continue operating under the garb of free expression while the survivors face the consequences.

SUGGESTIONS TO FILL THE LEGAL AND POLICY GAPS

The following suggestions should be followed to fill the legal and policy gaps in the protection of survivors of domestic violence from digital privacy violations:

1. Indian Cyber Laws to Be Strengthened for Digital Privacy Protection

The PWDVA, 2005, should be amended to include specific digital privacy protections, such as:

- Confidentiality of survivor identities in legal proceedings and social media complaints.
- Provisions for protection against cyberstalking, doxxing, and unauthorized data exposure.
- Specific punitive actions for the harasser.

2. Amending the IT Act, 2000 to include the following:

- Doxxing and disclosure of survivor's identities as an offense liable to be punished.
- Survivor-centric cyberstalking legislation that includes patterns of online abuse by known perpetrators.
- Compulsory removal of non-consensual intimate images within 24 hours of reporting.
- Create a specific category in the Bhartiya Nyaya Sanhita, 2023 to deal with digital abuse issues concerning domestic violence, thus penalizing online harassment and threats much more severely.

3. Bringing in Confidentiality and Survivor-Centric Legal Protections

Implement a Confidential Address Program like that of the United States' Safe at Home Program for survivors to have the option of:

- Using a legal substitute address for government-related agencies, banks, and their social media profiles.
- Maintaining their home addresses and personal information strictly confidential and unavailable for public viewing.

4. Ensure court proceedings are kept anonymous by:

- Survivors may file complaints with their names masked.
- Court records in domestic violence cases should be sealed and made inaccessible to other parties.
- Limit the media's freedom to publish survivors' identities unless consent is explicit.

5. Hold Social Media Companies Accountable

Make social media companies obligate stronger privacy protection for survivors by:

- Including "Survivor Mode" as privacy settings in their profiles which limit profile viewership, inhibit location tracking, and block contact.
- Improving AI-based moderation tools to identify and remove doxxing, cyberstalking, and revenge porn content more quickly.
- Automated removal of non-consensual disclosures involving domestic violence.

6. Strengthen reporting and response mechanisms by:

- Ensuring that platforms respond to abuse reports within 12–24 hours.
- Allowing survivors direct access to human moderators rather than automated responses.
- Developing a crisis response team to help survivors remove harmful content and secure their accounts.

7. Legal penalties for non-compliance:

- Imposing penalties on social media companies that do not take action against privacy violations.
- Creating a legal requirement for companies to notify survivors of possible privacy violations in real-time.

8. Strengthening Law Enforcement and Judicial Response

Train law enforcement officers to respond to digital privacy violations in domestic violence cases, including:

- Cyberstalking and doxxing as a serious threat to survivor safety.
- Responding promptly to social media-related threats and privacy breaches.

- Providing legal and digital security support to survivors.
9. Dedicated cybercrime units across all the states to:
- Investigate cases about online harassment, doxxing, and revenge porn against domestic violence survivors.
 - Collaboration with social media platforms for expedient removal of objectionable content.
 - Quick judicial process against digital abusers.
 - Setting up specific courts dealing with cyber cases of gender crimes
 - In cases of digital abuse within the domestic violence context
 - Faster disposal of cases so that justice can be served in time
 - Assist the survivor with gathering digital evidence.
10. Public Education and Digital Literacy Initiatives
- Public awareness campaigns on:
 - Dangers of privacy violations in social media to survivors of domestic violence.
 - The need for secure online behavior and digital self-defense.
 - Reporting cybercrimes and getting legal help.
 - Creating survivor-centric digital safety materials such as:
 - Digital security workshops for survivors, like how to control privacy settings, track digital footprints.
 - Kit for securing personal data and how to prevent surveillance by an abuser online.
 - Legal helplines and mobile apps dedicated to digital abuse assistance.

CONCLUSION

The digital age has transformed communication, socialization, and information sharing, yet it has also exposed domestic violence survivors to serious privacy risks. Social media, while providing a space for advocacy and support, has also become a tool for harassment, cyberstalking, doxxing, and unauthorized exposure of survivor identities. Despite legal protections under Article 21 of the Indian Constitution, the Protection of Women from Domestic Violence Act, 2005 (PWDVA), the Information Technology (IT) Act, 2000, and the Digital Personal Data Protection Act, 2023, significant gaps remain in the legal framework governing digital privacy and security for survivors.

The failure of social media companies to implement effective reporting systems, survivor-specific privacy settings, and content moderation mechanisms further exacerbates these risks. Survivors who turn to social media for support often find themselves exposed to public scrutiny, cyber harassment, and online vigilantism, making it difficult to escape digital abuse. While some countries have stronger legal protections, including confidential address programs and strict anti-doxxing laws, India still lacks comprehensive legislation that explicitly addresses the intersection of domestic violence and digital privacy violations.

To ensure the protection and dignity of survivors, legal reforms must focus on strengthening cyber laws, improving enforcement mechanisms, increasing social media accountability, and raising public awareness. A collaborative approach involving legal authorities, policymakers, tech companies, and civil society organizations is essential to safeguard survivor privacy in the digital era.

REFERENCES

1. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
2. Protection of Women from Domestic Violence Act, 2005, No. 43 of 2005 (India).
3. Information Technology Act, 2000, No. 21 of 2000 (India).
4. Indian Penal Code, 1860, Act No. 45 of 1860 (India).
5. International Journal of Law and Cyber Crime, "Privacy and Digital Harassment: The Growing Threat to Domestic Violence Victims in India," 2022, 34(2).
6. European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

7. Digital Civil Rights Movement, "The Rise of Doxxing: A Digital Danger for Domestic Violence Survivors," 2021.
8. Digital Personal Data Protection Act, 2023, No. 13 of 2023 (India).
9. "Digital Personal Data Protection Act: Social Media Users Under 18 to Require Parental Consent," *The Economic Times* (Jan. 4, 2024, 10:30 AM), <https://economictimes.indiatimes.com/news/india/digital-personal-data-protection-act-social-media-users-under-18-to-require-parental-consent/articleshow/116925617.cms?from=mdr>.
10. **"Right to Privacy & Social Media,"** *TSCLD* (last visited Jan. 23, 2025), <https://www.tsclld.com/right-to-privacy-social-media>.
11. "Navigating Privacy and Security: Human Rights in the Digital Age," *Drishti Judiciary* (last visited Jan. 23, 2025), <https://www.drishtijudiciary.com/blog/navigating-privacy-and-security-human-rights-in-the-digital-age>.
12. "The Right to Privacy in the Digital Age," *LawVS* (last visited Jan. 23, 2025), <https://lawvs.com/articles/the-right-to-privacy-in-the-digital-age>.
13. "Social Media Regulation for Children," *Drishti IAS* (last visited Jan. 23, 2025), <https://www.drishtiias.com/daily-updates/daily-news-analysis/social-media-regulation-for-children>.