THE LAWWAY WITH LAWYERS JOURNAL
VOLUME:-26 ISSUE NO:- 26 , AUGUST 15, 2025
ISSN (ONLINE):- 2584-1106
Website: www.the lawway with lawyers.com
Email: thelawwaywithelawyers@gmail.com
Authored By : Aritra Biswas

CYBERCRIMES, WOMEN'S SAFETY, AND CHILD PROTECTION: A COMPREHENSIVE ANALYSIS OF LEGAL FRAMEWORKS, CHALLENGES, AND REMEDIAL STRATEGIES

Abstract

The pervasive digitalization of modern life has ushered in an era of unprecedented connectivity alongside a complex landscape of cybercrime. This paper critically examines the escalating threat of cybercrimes, with a particular focus on their disproportionate impact on women and children, who face severe psychological, social, and financial consequences. It delineates various types of cybercrime, from hacking and malware to online child sexual exploitation and non-consensual image sharing, supported by global prevalence statistics highlighting the immense scale and economic toll of these illicit activities. The study provides a comprehensive overview of existing legal and policy responses, including international conventions like the UN Convention against Cybercrime, the Budapest Convention, and the Istanbul Convention, as well as national frameworks, with a specific emphasis on India's Information Technology Act and the POCSO Act. Furthermore, it identifies multifaceted challenges in enforcement and prosecution, such as the borderless nature of the internet, perpetrator anonymity, complexities of digital evidence, and critical gaps in digital literacy and societal awareness. Concluding with a synthesis of preventative measures and best practices, the paper advocates for a holistic, multi-stakeholder, and adaptive approach, integrating legal reforms, technological safeguards, and comprehensive social and educational interventions to foster a safer and more equitable digital environment for vulnerable populations.
Keywords: Cybercrime, Women's Safety, Child Protection, Legal Remedies, Digital Violence, Online Harassment, Child

Sexual Exploitation, Cybersecurity, International Law, Indian Law, Digital Forensics, Prevention, Awareness, Technology-Facilitated Violence.

1. Introduction

The digital age, characterized by the pervasive integration of information and communication technologies (ICTs) into nearly every facet of daily life, has profoundly transformed global communication, commerce, and social interaction. This rapid digitalization, while offering unprecedented opportunities for connectivity and development, has simultaneously opened new and complex avenues for criminal activity. Cybercrime, broadly defined as criminal activities carried out using computers, networks, or other digital devices, is a rapidly evolving threat that exploits security vulnerabilities at both individual and enterprise levels.[^1, ^2] The inherent borderless nature of the internet allows cybercriminals to operate globally, often with a significant degree of anonymity, posing unprecedented challenges for traditional law enforcement and established legal frameworks.[^3, ^4]

Within this evolving digital landscape, the safety and protection of vulnerable populations, particularly women and children, have emerged as critical concerns. These groups are disproportionately targeted by specific forms of cybercrime, experiencing severe and often lasting harm that extends beyond the digital realm into their physical, psychological, and social well-being.[^5, ^6, ^7] The pervasive nature of online violence can lead to profound distress, isolation, and economic hardship, fundamentally impacting their ability to participate fully and safely in society. Consequently, ensuring their safety online is not merely a matter of technological cybersecurity but represents a fundamental human rights issue, crucial for fostering inclusive and equitable digital environments.[^6, ^8]

This paper aims to provide a holistic understanding of the intricate nexus between cybercrimes, women’s safety, and child protection. It offers a critical review of current responses, including existing international and national legal frameworks, and identifies pathways for more effective intervention. The subsequent sections will detail the types and prevalence of cybercrime, their specific impacts on women and children, the existing legal and policy landscape, the multifaceted challenges in enforcement and prosecution, and a synthesis of preventative strategies and recommendations.

2. The Evolving Landscape of Cybercrime

2.1. Defining Cybercrime: Types and Modus Operandi

Cybercrime encompasses a diverse array of illicit activities, ranging from financially motivated attacks to those directly targeting personal safety and privacy. These crimes exploit digital vulnerabilities and human behavior, often employing sophisticated methods. Common types of cybercrime include:

- **Hacking:** This involves gaining unauthorized access to computer systems or networks. Perpetrators exploit system weaknesses to steal sensitive data, ranging from personal information and corporate secrets to government intelligence, or to disrupt operations of companies and governments. Such intrusions cost billions of dollars annually.[^9, ^10]
- **Malware:** Malicious software, including viruses, worms, trojans, adware, spyware, and ransomware, is designed to interfere with a computer's normal functioning or to commit cybercrimes. Ransomware, a particularly insidious type, encrypts valuable digital files and demands a ransom for their release, often infiltrating systems via deceptive emails.[^1, ^9, ^10]
- **Identity Theft:** This occurs when an individual unlawfully obtains and uses another person's personal information, such as credit card numbers, social security numbers, or dates of birth, to commit theft or fraud. While not all identity thefts are cyber-attacks, malware (like trojans and spyware) and phishing are frequently employed to steal such data.[^1, ^9, ^10]
- **Social Engineering:** This psychological manipulation technique tricks people into performing actions or divulging confidential information. Cybercriminals use social engineering to commit online fraud, often establishing trust through platforms like online dating sites before soliciting money or information. This technique is frequently combined with technological elements, such as deceptive messaging in phishing attempts.[^1, ^9]
- **Phishing and Email Scams:** These are misleading schemes that use fake emails or texts to mimic trusted sources (e.g., banks, well-known companies) and deceive recipients into providing sensitive information or clicking malicious links that install malware.[^1, ^9, ^10]
- **Social Media Fraud:** Scams that leverage social media platforms (Facebook, Twitter, Instagram, TikTok) to defraud victims. Examples include fictitious online stores, "catfishing" (creating fake online identities), social engineering attacks, or impersonation scams. These frauds often exploit user trust and a tendency to overshare personal information.[^1, ^10]

- **Cyberbullying:** Also known as online or internet bullying, this involves sending or sharing harmful, humiliating, or intimidating content about someone else. It is particularly common among teenagers and can cause embarrassment, psychological problems, and in extreme cases, lead to suicide.[^5, ^10]
- **Cyberstalking:** Defined as unwanted persistent online contact from someone targeting individuals with the aim of controlling or intimidating them, such as continuous unwanted calls and messages.[^1, ^10]
- **Online Drug Trafficking & Electronic Money Laundering:** The rise of cryptocurrency and the "Dark Web" has facilitated secure and private online drug deals and money laundering, making it easier to transfer illicit funds without drawing law enforcement attention.[^10]
- **Cyber Extortion:** This involves cybercriminals demanding money to return stolen data or to cease malicious activities, such as denial-of-service (DoS) attacks.[^10]
- **Non-Consensual Image Sharing (Revenge Porn):** The online release of explicit photographs or videos of an individual without their permission, primarily for the purpose of humiliation. These images are often initially shared voluntarily within intimate relationships.[^11]

The diverse range of cybercrimes highlights a crucial observation: the digital realm is not merely a new venue for traditional criminal activities, but a transformative tool that fundamentally reshapes criminal methodologies. For instance, while "social engineering" is a psychological tactic, its online application through phishing or catfishing transforms it into a cybercrime. Similarly, human trafficking or money laundering, historically physical crimes, are amplified and streamlined by digital means, blurring the lines between "cybercrime" and "traditional crime".[^1, ^12] This blurring necessitates a holistic legal and policy response that integrates digital considerations into all aspects of criminal justice, rather than siloing cybercrime as a separate category. Effective prevention strategies must therefore address both technical vulnerabilities and human behavioral susceptibilities.

Table 1: Common Cybercrimes and Modus Operandi

Crime Type	Brief Definition	Modus Operandi/Examples	Primary Impact
Hacking	Unauthorized access to computer systems or networks.	Exploiting system weaknesses to steal data (personal, corporate secrets, government intelligence) or disrupt operations.	Data t operational disruption, fina loss.

Crime Type	Brief Definition	Modus Operandi/Examples	Primary Impact
Malware	Malicious software designed to interfere with computer functioning.	Viruses, worms, trojans, adware, spyware, ransomware. Often delivered via email attachments or malicious websites.	System damage, theft, data encryp (ransomware), disrupted productivity, financial loss.
Identity Theft	Unlawfully obtaining and using personal information for fraud.	Using malware (trojans, spyware) or phishing to steal SSNs, credit card details, dates of birth, online account credentials.	Financial damaged cr emotional distres
Social Engineering	Psychological manipulation to divulge confidential information or perform actions.	Online dating scams, phishing messages using deceptive stories to gain trust and solicit money/information.	Financial fr information disclosure.
Phishing & Email Scams	Deceptive communications mimicking trusted sources.	Fake emails/texts (e.g., from banks, well-known companies) tricking recipients into clicking malicious links or revealing sensitive data.	Information t financial malware infectio
Social Media Fraud	Scams exploiting social media platforms.	Fictitious online stores, catfishing, impersonation scams, social engineering attacks.	Financial fr identity t emotional distres
Cyberbullying	Sending or sharing harmful, humiliating, or intimidating content online.	Posting embarrassing photos/videos, spreading rumors, sending threatening messages.	Psychological distress, s isolation, acad difficulties, harm, suicide.
Cyberstalking	Persistent unwanted online contact for intimidation or control.	Repeated unwanted calls/messages, online harassment, tracking movements using GPS.	Fear, anx emotional dist physical unsafety
Non-Consensual	Online release of explicit	Sharing intimate photos/videos taken in	Humiliation, reputational dam

Crime Type	Brief Definition	Modus Operandi/Examples	Primary Impact
Image Sharing	images/videos without permission.	private without consent, often by ex-partners.	psychological trauma, job suicidal thoughts

2.2. Global Trends and Statistics

Cybercrime represents a rapidly escalating global threat with profound economic and social consequences, affecting individuals, businesses, and governments worldwide.

The sheer scale of its impact is staggering. In 2022, a minimum of 422 million individuals were affected by cybercrime, with over 800,944 complaints registered globally.[^13] The year 2023 alone saw nearly 33 billion accounts breached, translating to an alarming rate of 97 cybercrime victims every hour.[^13, ^14] On average, a hacker attack occurs every 39 seconds.[^13]

The financial toll of cybercrime is immense and continues to grow exponentially. The global annual cost of cybercrime is projected to reach an astounding $10.5 trillion by 2025, a significant increase from $8 trillion in 2023.[^13, ^14] Cybercriminals collectively earn an estimated $1.5 trillion every year.[^13] Ransomware, a particularly destructive form of cybercrime, is predicted to cost its victims around $265 billion annually by 2031.[^13] For businesses, the average cost of a data breach was $4.35 million in 2022, further escalating to $4.88 million in 2024.[^14]

Analysis of prevalent attack vectors reveals consistent patterns. Phishing remains the most common form of cybercrime, accounting for approximately 80% of reported cybercrimes and 41% of data security incidents in 2023.[^13, ^14] Ransomware attacks also demonstrated widespread impact, affecting 72.7% of companies globally in 2023.[^13] A critical vulnerability across many cyber incidents is the human element, which factored into 82% of breaches against businesses, often through sophisticated social engineering tactics.[^13, ^14]

The COVID-19 pandemic significantly exacerbated the cybercrime landscape, leading to a 69% increase in victim count in 2020 compared to 2019.[^13, ^14] The number of victims under 20 years old doubled during this period, likely due to increased online studying and digital engagement.[^13] Small and medium-sized businesses (SMBs) are particularly vulnerable, accounting for 43% of annual cyberattacks.[^13] The healthcare industry has consistently been a prime target, suffering more data breaches than any other sector for 13 consecutive years.[^13]

Geographically, Asia (26%), Europe (24%), and North America (23%) experienced the most cyberattacks in 2021.[^14] The United Kingdom reported the highest density of cybercrime victims per million internet users (4783 in 2022), followed by the USA (1494).[^14]

The immense financial scale of cybercrime, with annual costs in the trillions, indicates that these activities are not merely opportunistic but constitute a highly profitable and increasingly organized industry. The emergence of "crimes-as-a-service" and the availability of "off-the-shelf" hacking tools suggest a professionalized and accessible criminal ecosystem.[^12, ^15] This professionalization implies that traditional law enforcement methods, which are often reactive and localized, are increasingly insufficient. A coordinated, proactive, and globally integrated approach is required, one that mirrors the sophistication and cross-border nature of these criminal enterprises. Such an approach must also consider economic disincentives and strategies to disrupt criminal supply chains.

Furthermore, the escalating number of cybercrime victims and associated costs is directly linked to the widespread increase in internet usage, particularly evident during the pandemic. The significant role of the human element in breaches highlights a critical paradox: while digital connectivity offers vast opportunities, it simultaneously expands the "attack surface" and human vulnerability.[^13, ^14] This suggests that simply enhancing cybersecurity *technology* is not enough. Effective solutions must also focus on human factors, including digital literacy, robust awareness campaigns, and fostering a pervasive culture of online safety.[^16, ^17] The continuous and rapid evolution of technology also means that new vulnerabilities are constantly emerging, necessitating continuous adaptation of security measures and legal frameworks to remain effective.[^18]

Table 2: Global Cybercrime Statistics and Costs

Metric	Latest Figure/Projection	Year/Source
Individuals Impacted	422 million minimum	2022 (FBI) [^13]
Complaints Registered	800,944	2022 (FBI) [^13]
Accounts Breached	Nearly 33 billion	2023 [^13]
Cybercrime Victims per Hour	97	2023 [^13, ^14]

Metric	Latest Figure/Projection	Year/Source
Hacker Attack Frequency	Every 39 seconds	Projected 2025 [^13
Global Annual Cost of Cybercrime	$10.5 trillion	Projected 2025 [^14]
Ransomware Annual Cost	$265 billion	Predicted by 2031 [
Cybercriminals' Annual Earnings	$1.5 trillion	[^13]
Average Cost of Data Breach (Businesses)	$4.88 million	2024 [^14]
Phishing Prevalence (of reported cybercrimes)	80%	[^13]
Companies Affected by Ransomware	72.7%	2023 [^13]
Breaches Involving Human Element	82%	[^13, ^14]
SMBs Targeted by Cyberattacks	43%	Annually [^13]
Increase in Victim Count (COVID-19)	69% (2020 vs. 2019)	[^13, ^14]
UK Victims per Million Internet Users	4783	2022 [^14]
USA Victims per Million Internet Users	1494	2022 [^14]

3. Impact on Vulnerable Populations: Women and Children

3.1. Impact on Women's Safety

Online violence against women and girls (VAWG) is a rapidly escalating global problem with profound and far-reaching consequences that often extend from the digital sphere into offline realities.[^5, ^6] This phenomenon results in significant physical, sexual, psychological, and financial harm.

The **psychological consequences** are particularly severe. Victims frequently experience paranoia, intense shame, social isolation, diminished self-esteem, and pervasive mental and emotional stress. These can manifest as depression and anxiety, and in extreme cases, lead to suicidal thoughts or even suicide.[^5, ^11, ^19, ^20] The enduring nature of digital content, once posted online, combined with societal stigmatization, significantly amplifies these psychological impacts, creating a continuous cycle of distress.[^5] For instance, victims of non-consensual image sharing (often termed "revenge porn") report experiencing severe emotional distress (affecting 80% to 93% of

victims), alongside anger, guilt, and paranoia, often leading to lifelong mental health struggles.[^11, ^19]

Social consequences include a chilling effect on women's online participation. Online violence can force women to self-censor their opinions, deactivate social media accounts, or withdraw entirely from digital spaces, thereby widening the digital gender gap and diminishing their voices in essential public and professional spheres.[^5] Victims of non-consensual image sharing frequently report a profound loss of dignity, diminished respect from family and friends, and increased social isolation.[^11, ^19] A pervasive issue is victim blaming, where individuals are often perceived as promiscuous and held responsible for the abuse they suffer, reflecting a harmful sexual double standard.[^19] Furthermore, online harassment can escalate into real-world physical threats, stalking, and even violence, leading to heightened anxiety and significant changes in daily behavior as victims attempt to protect themselves.[^21]

The **financial consequences** are also substantial. Women targeted by cybercrimes, particularly phishing attacks, have experienced extortion, identity theft, and significant economic damages, including being manipulated into paying for fraudulent services.[^5] Identity theft, regardless of how it is perpetrated, can cause severe financial harm, impacting credit scores and long-term financial stability.[^22]

Specific forms of online violence disproportionately affect women. **Online harassment and cyberbullying** are highly prevalent, with one in four American women reporting having experienced online abuse. Cyberbullying (10%) and sexual harassment (9%) are the most frequent types reported.[^21] Demographic data indicates that women of color, especially those with mixed racial backgrounds (37%) and Latina/Hispanic women (31%), experience higher rates of online abuse.[^21] Younger women, aged 18-34, are also at a demonstrably higher risk across various forms of online abuse.[^21] **Non-consensual image sharing (revenge porn)** is a particularly gendered crime, with 90% of victims being women. Its consequences can be devastating, including job loss, persistent stalking and harassment, "doxxing" (publicly exposing private information), and in severe cases, the necessity of changing one's identity due to prolonged online torment.[^19] This form of sexually-motivated online abuse is explicitly identified as disproportionately affecting women.[^21] Emerging threats like **AI deepfakes**, though relatively new, already affect 2% of

women surveyed, with 70% of affected victims reporting severe or significant negative impacts.[^21] The broader category of **Technology-Facilitated Gender-Based Violence (TFGBV)** encompasses these harms, with studies suggesting that between 16% and 58% of women globally have experienced some form of TFGBV. This includes doxing, deepfake abuse, and the exacerbation of existing forms of violence such as sexual harassment and stalking through digital means.[^23, ^24, ^25]

The consistent patterns observed suggest that online violence against women is not a novel phenomenon but rather an amplification and extension of existing gender-based violence and inequalities. The persistence of a sexual double standard, where women are judged more harshly for comparable sexual behavior, and the disproportionate targeting of women of color and younger women, illustrate how pre-existing societal biases are mirrored and magnified in the digital sphere.[^5, ^6, ^19, ^21, ^23] This digital amplification of gender inequality underscores the critical need for gender-sensitive approaches in policy development, content moderation, and support services. Without explicitly recognizing and addressing the gendered nature of these harms, interventions risk being ineffective or even perpetuating existing disparities.

3.2. Impact on Child Protection

Children, due to their inherent vulnerabilities, developmental stage, and increasing digital engagement, are particularly susceptible to cybercrimes, experiencing serious and often long-lasting harm.

The **psychological consequences** for child victims are profound. They frequently experience intense fear and anxiety, a deep loss of trust in technology and adults, and can develop post-traumatic stress disorder (PTSD).[^7, ^22] Long-term effects include chronic stress, depression, and anxiety, which can lead to insomnia, irritability, and difficulty concentrating.[^22, ^26] The permanence of online images of abuse, particularly in cases of online child sexual exploitation, intensifies PTSD and creates a continuous sense of insecurity and exposure, compounding psychological distress.[^7] Shame and guilt are pervasive emotions, often reinforcing the fear of revealing abuse and leading to panic attacks, sleep disorders, and concentration problems.[^7] In severe cases of cyberbullying, young people have experienced self-harm and suicidal ideation, with studies indicating a 50% increased risk of suicidal thoughts for adolescents exposed to cyberbullying.[^26, ^27]

Social consequences include significant isolation. Children who are bullied online often withdraw from peers, family, and friends, spending excessive time alone and avoiding school.[^26] Victims of online child sexual exploitation may experience relational difficulties, struggling to establish and maintain intimate and friendly relationships due to the betrayal and manipulation they have endured.[^7] This can be devastating to their academic and social development, potentially leading to poor grades and school dropouts.[^26, ^28]

The **financial consequences** for child victims, while sometimes indirect, can be substantial. Identity theft can cause significant financial and emotional harm, and financial sextortion directly targets children for monetary gain.[^22, ^29] Damage to reputation, though not always financial, can have lasting social and economic impacts.

Specific forms of cybercrime severely impact children:

- **Online Child Sexual Exploitation and Abuse (OCSEA):** This is a major and escalating component of cybercrime, encompassing a wide array of offenses like child sexual exploitation material (CSEM), online grooming, sexting, sextortion, and livestreaming of sexual abuse.[^7] The "Global Threat Assessment 2023" reported an 87% increase in child sexual abuse content since 2019, with the National Center for Missing & Exploited Children (NCMEC) receiving over 32 million reports in 2022.[^7] New digital technologies, particularly Artificial Intelligence (AI), are making it easier for criminals to create and disseminate abusive content and evade detection.[^7] In 2024, NCMEC's CyberTipline saw a 1,325% increase in reports involving Generative AI.[^29] Financial sextortion is a growing concern, with NCMEC receiving nearly 100 reports daily in 2024, and since 2021, over three dozen teenage boys have died by suicide as a result of this crime.[^29] Globally, one in twelve children (8%) has been subjected to online child sexual exploitation or abuse, with online solicitation (12.5%) and non-consensual image sharing (12.6%) being common subtypes.[^30] Livestreaming of child sexual abuse, often facilitated by close individuals for money, poses a high risk of revictimization due to continuous online dissemination.[^7]
- **Cyberbullying:** This is a prevalent issue, with over a third of young people in 30 countries reporting being cyberbullied, and one in five skipping school as a result.[^31] It can lead to emotional and physical harm, loss of self-esteem, shame, anxiety, and difficulties with concentration and learning.[^27] Cyberbullying can also violate children's human rights, including the right to physical and mental health, freedom of expression, leisure, and education.[^27]

The prevalence and severity of cybercrimes against children highlight a critical exploitation of child vulnerabilities in the digital realm. Children's developing brains, coupled with the anonymity and accessibility offered by online platforms, make them prime targets for manipulation, grooming, and abuse.[^5, ^7] The ease with which perpetrators can operate across borders and hide their identities exacerbates this vulnerability. This situation necessitates comprehensive protection strategies that go beyond mere technical safeguards to address the psychological, social, and developmental aspects of child safety online.

Furthermore, the impact of these cybercrimes demonstrates the profound interconnectedness of online and offline harm. Digital abuse, though occurring in an immaterial environment, has very real and devastating consequences in the physical world, affecting mental health, relationships, and daily life.[^7, ^26, ^32] This means that interventions cannot be confined to the digital sphere but must adopt a holistic approach that recognizes how online experiences can exacerbate existing offline vulnerabilities, such as domestic violence or school bullying.[^7] A comprehensive response requires bridging the gap between digital safety initiatives and broader child protection and mental health services.

4. Legal Remedies and Frameworks

4.1. International Legal Frameworks and Conventions

The global nature of cybercrime necessitates a robust international legal framework to facilitate cooperation and ensure accountability across jurisdictions. Several key conventions and organizations contribute to this effort:

- **United Nations Convention against Cybercrime (UN Convention):** Adopted by the UN General Assembly on December 24, 2024, this is the first comprehensive global treaty specifically addressing cybercrime. It provides states with a range of measures to prevent and combat cybercrime and aims to strengthen international cooperation in sharing electronic evidence for serious crimes. The Convention's nine chapters offer a comprehensive approach while incorporating human rights safeguards, adjusting traditional criminal investigation methods to the ICT environment, and enhancing international cooperation.[^33] The Convention is set to open for signature on October 25, 2025, in Hanoi, Viet Nam.[^33]
- **Council of Europe Convention on Cybercrime (Budapest Convention):** This is the most relevant international legally binding

treaty on cybercrime and electronic evidence. It requires signatory parties to criminalize offenses against and by means of computer data systems, including child pornography, computer-related fraud, and copyright infringements. It also establishes procedural law tools for securing electronic evidence and a framework for international cooperation among parties. The Convention serves as a guideline for countries developing national cybercrime legislation and aims to reduce "safe havens" for criminals by harmonizing approaches.[^34, ^35, ^36]

- **Istanbul Convention (Convention on Preventing and Combating Violence against Women and Domestic Violence):** While not exclusively a cybercrime treaty, the Istanbul Convention is highly relevant for addressing online and technology-facilitated violence against women. It is the most far-reaching legally binding human rights treaty covering all forms of violence against women and domestic violence, recognizing its structural nature as gender-based violence. Its broad scope extends to violence committed in the digital space, with specific articles applicable to online sexual harassment (Article 40), stalking (Article 34), and psychological violence (Article 33). It also mandates due diligence from states to prevent, investigate, and punish acts of violence by non-state actors, which includes online violence.[^34, ^35] The Budapest Convention complements the Istanbul Convention by providing the specific tools for investigating and securing electronic evidence needed for prosecuting such technology-facilitated violence.[^34]
- **UN Convention on the Rights of the Child (CRC) and Protocols:** The CRC establishes fundamental obligations for states to protect, respect, and fulfill children's rights, including their right to be free from violence, exploitation, trafficking, cyberbullying, and privacy invasion in the digital environment.[^31, ^37] The UN Committee on the Rights of the Child, which monitors CRC implementation, has issued guidance on how children should be treated in the digital world and how their rights should be protected, including strong measures against harmful content and all forms of digital violence.[^31] Relevant optional protocols, such as the Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography, further strengthen these protections.[^37]
- **UNICEF's Role in Legislative Reform:** UNICEF actively works to reform national laws globally to keep pace with technology-facilitated crimes against children. For instance, UNICEF's technical support led to Zimbabwe's Data Protection Act in 2021, which criminalizes various forms of online violence against women and children. They also supported new legislation in the Philippines in 2022 to tackle online sexual abuse and exploitation and developed a global guide to enhance legislative frameworks based on international conventions.[^38]

- **Interpol and Europol's Role:** International police organizations like Interpol and Europol play crucial roles in combating cybercrime by fostering international cooperation, intelligence sharing, and operational coordination. Interpol's strategic analysis reports highlight the significant increase in the sophistication and volume of cyberattacks, including child sexual abuse and financial fraud.[^15] Europol collaborates with Eurojust to address persistent and emerging challenges in cybercrime investigations involving digital evidence, emphasizing the need for legal tools to alleviate these challenges.[^39] Both organizations provide platforms and services for secure information exchange and collaborative operations among law enforcement agencies worldwide.[^12, ^40]

The existence of multiple international conventions and initiatives addressing aspects of cybercrime, women's safety, and child protection creates a complex, and at times, fragmented legal landscape. While each instrument contributes valuable provisions and mechanisms, their varied scope, adoption rates, and interpretations across different nations can hinder a truly unified global response. This situation underscores the need for greater harmonization of legal definitions, enhanced cross-border enforcement mechanisms, and more seamless collaboration among international bodies to ensure comprehensive protection for vulnerable populations in the digital age.

4.2. National Legal Frameworks (Focus on India)

India has progressively developed its national legal framework to combat cybercrimes, with a particular focus on protecting women and children, recognizing that "Police" and "Public Order" are State subjects. The Central Government supplements the initiatives of States/Union Territories (UTs) through advisories and financial assistance.

- **Information Technology (IT) Act, 2000 and Amendments:** This Act serves as India's primary legislation governing cybercrimes, electronic transactions, and online communication. It provides legal recognition to electronic contracts, records, and signatures, and criminalizes various forms of cybercrime such as hacking and data breaches.[^41, ^42] Subsequent amendments have significantly strengthened its provisions, particularly those addressing crimes that violate the safety and dignity of women in online spaces. These amendments introduced stricter penalties and new provisions to tackle cyberstalking, voyeurism, the transmission of sexually explicit material, and the non-consensual distribution of private images. Key sections include 66E (penalizing unauthorized capture, publication, or transmission of private images without consent,

relevant for revenge pornography), 67 (criminalizing publication/transmission of obscene material), and 67A (specifically dealing with sexually explicit content).[^41, ^43, ^44]

- **Protection of Children from Sexual Offences (POCSO) Act, 2012:** This essential legislation specifically addresses sexual offenses committed against children. POCSO criminalizes various cybercrimes against children, including child pornography, cyberstalking, cyberbullying, defamation, grooming, hacking, identity theft, online child trafficking, online extortion, sexual harassment, and violation of privacy.[^43, ^45] The Act is gender-neutral, applying to both male and female victims and offenders under 18 years of age. It not only outlines punishments but also establishes a system for victim support, child-friendly provisions for recording statements and evidence, and ensures speedy trials.[^43, ^45]
- **Indian Cyber Crime Coordination Centre (I4C) and National Cyber Crime Reporting Portal (NCRP):** Established by the Ministry of Home Affairs, the I4C acts as a central attached office to deal with all types of cybercrimes in a coordinated and comprehensive manner.[^42] As part of I4C, the National Cyber Crime Reporting Portal (https://cybercrime.gov.in) was launched to enable the public to report cybercrime incidents, with a special focus on crimes against women and children. Incidents reported on this portal are routed to the respective State/UT Law Enforcement Agencies for conversion into FIRs and subsequent action.[^42, ^44] A toll-free helpline number, 1930, has also been operationalized for assistance in lodging online complaints.[^43]
- **Other Initiatives:** India has also established **National Cyber Forensic Laboratories** (one for evidence in Hyderabad, inaugurated 2022, and one for investigation in New Delhi) to provide forensic support, preserve evidence, and reduce turnaround times in cybercrime cases.[^42, ^44] The **Cyber Fraud Mitigation Centre (CFMC)** at I4C brings together representatives from banks, financial intermediaries, and telecom providers for immediate action against cyber fraud.[^42] **Joint Cyber Coordination Teams (JCCTs)** have been constituted in cybercrime hotspots to enhance coordination among State/UT LEAs.[^44] Furthermore, the government actively conducts extensive **awareness campaigns** through SMS, social media (e.g., @CyberDost), radio, and various publications to educate the public, including women and children, about cyber safety and crime prevention.[^42, ^43, ^44]

While national laws like the IT Act and POCSO Act are progressive, their effective implementation faces significant challenges. These challenges include the rapid pace of technological change, which can quickly render legal provisions

outdated, and the need for robust enforcement mechanisms across diverse states and union territories. The reliance on state-level law enforcement for investigation and prosecution, despite central government support, can lead to inconsistencies in application and outcomes. This situation highlights the continuous need for legal frameworks to evolve in tandem with technological advancements and for consistent capacity building and resource allocation across all levels of law enforcement.

4.3. Case Studies (India)

Case studies from India illustrate the real-world impact of cybercrimes on women and children and the ongoing challenges in achieving justice through existing legal frameworks.

Cybercrime Against Women:

- **Ritu Kohli Case:** This is recognized as one of the earliest recorded instances of cyberstalking in India. The victim reported that someone was using her identity online, disclosing her personal information, and using profane language, leading to numerous unwanted calls. Authorities tracked the IP address and arrested Manish Kathuria. A complaint was filed under Section 509 of the Indian Penal Code (IPC) for insulting a woman's modesty. However, this case exposed a significant legal gap: Section 509 IPC primarily applied to words, gestures, or physical acts and did not explicitly cover equivalent actions performed online. This deficiency prompted the introduction of Section 66A of the Information Technology Act of 2008, which established penalties for sending inflammatory statements via telecommunications services, including imprisonment.[^46] This case underscored the imperative for legal frameworks to adapt to new forms of digital harassment.
- **Sulli Deals and Bulli Bai Case:** These recent cases highlight the severe nature of online harassment targeting women, particularly Muslim women, in India. The "Sulli Deals" platform, established in July 2021, and the "Bulli Bai" application, developed later, were used to "list" and "auction" Muslim women online, referring to them as "bargains of a day." These incidents, which involved the non-consensual use of women's images and identities for derogatory purposes, garnered widespread outrage and media attention. Mumbai and Delhi police collaborated, alongside the Cyber Emergency Reaction Group, India, to identify and apprehend the perpetrators. These cases exemplify the potential for online platforms to be weaponized for large-scale, targeted harassment and the critical need for effective legal and enforcement responses to protect vulnerable communities.[^46]

Cybercrime Against Children:

- **Delhi High Court Ruling (2016 Cyber-bullying Case):** A significant ruling by the Delhi High Court in a 2016 cyber-bullying case underscored the severe psychological impact of digital abuse on minors. The case involved a 14-year-old girl who received a morphed nude image with her face superimposed on another body, accompanied by threats to post the content on Facebook unless she complied with demands. Justice Swarana Kanta Sharma described this as a "textbook example of cyber-bullying," emphasizing that such virtual conduct has "very real and devastating consequences." The court noted that the psychological impact on a minor from faceless and silent digital abuse can be as mentally scarring as physical violence and is difficult to quantify. The accused was convicted under relevant provisions of the Indian Penal Code, the Protection of Children from Sexual Offences Act, and the Information Technology Act, and sentenced to five years of rigorous imprisonment. The High Court upheld the conviction, stressing the importance of effectively detecting and punishing such crimes to uphold a child's right to safety, dignity, and mental well-being.[^32]
- **Uninor Survey on Cyber Harm (India):** A survey conducted by Uninor in schools across seven Indian states revealed that 30% of Indian children accessing the internet have experienced some form of cyber harm. This includes prevalent issues such as cyberbullying, cyberstalking, hacking, and defamation. The survey highlights the widespread vulnerability of school children to online threats and the critical need for increased awareness and protective measures.[^28]

These case studies collectively illustrate the ongoing struggle to translate legal frameworks into effective prosecution and victim redressal. The Ritu Kohli case demonstrated early legal gaps, while the Sulli Deals and Bulli Bai cases highlighted the persistent challenge of large-scale online harassment and the need for swift, coordinated law enforcement action. The Delhi High Court ruling, while a positive step in recognizing the severe psychological impact on children and imposing a conviction, also underscores the complex nature of digital evidence and the need for specialized legal and forensic expertise. These examples reveal that despite legislative efforts, technological complexities, the anonymity of perpetrators, victim reluctance to report due to fear or shame, and limitations in enforcement capacity continue to pose significant barriers to achieving justice.

5. Challenges in Enforcement and Prosecution

The prosecution of cybercrimes, particularly those targeting women and children, is fraught with complex challenges that span legal, jurisdictional, and non-legal dimensions. These difficulties often impede effective investigation, evidence collection, and successful conviction.

5.1. Legal and Jurisdictional Challenges

- **Borderless Nature of Cybercrime:** Cybercrime inherently transcends national borders, creating significant complexities in determining which country has the authority to prosecute and which laws apply. A single attack might involve perpetrators coordinating from multiple countries, malicious infrastructure hosted across various jurisdictions, and victims located worldwide.[^3, ^12, ^37, ^47, ^48, ^49] This multi-jurisdictional aspect necessitates careful navigation of differing federal and state laws within a single country, let alone across international boundaries.
- **Anonymity of Perpetrators:** The internet provides a significant degree of anonymity, making it exceedingly difficult to identify and apprehend cybercriminals. Techniques such as encryption, the use of Virtual Private Networks (VPNs), and the dark web further complicate the task of tracing criminal activities to their source.[^4, ^47] This anonymity empowers perpetrators, as they do not need to be physically close to their victims to commit a crime.[^4]
- **Lack of Harmonized Laws:** Varying national legal frameworks for cybercrime, differing widely in their definitions, scope, and enforcement mechanisms, impede effective international cooperation. This lack of homogeneity can create “safe havens” for criminals in jurisdictions with less stringent laws or weaker enforcement capabilities.[^36, ^47]
- **Extradition Difficulties:** The complexities of extraditing suspects across international borders are a significant hurdle. Determining which laws apply and how to compel the surrender of individuals from one country to another for prosecution can be a protracted and challenging process, often hindering the pursuit of justice.[^47]

5.2. Digital Evidence Challenges

Digital evidence is central to cybercrime prosecution, yet its unique characteristics present numerous difficulties for law enforcement and judicial systems.

- **Collection, Preservation, and Admissibility:** The volatility of digital evidence makes its collection and preservation particularly challenging. Data can be easily altered, corrupted, or lost, requiring specialized tools and techniques to gather it without compromising its integrity. Ensuring that digital evidence meets stringent legal standards for admissibility in

court is paramount; any indication of tampering or improper handling can undermine a case.[^47, ^50, ^51, ^52]

- **Chain of Custody:** Maintaining a meticulous chain of custody for digital evidence is critical to proving its integrity and authenticity in court. This involves thoroughly documenting every individual who has handled the evidence, the time and place of collection, storage location, and access logs. Gaps or inconsistencies in the chain of custody can lead to the evidence being deemed unreliable or inadmissible.[^47, ^50, ^51, ^52]
- **Volume and Diversity of Data:** The exponential increase in digital evidence, originating from a multitude of diverse devices (smartphones, CCTV, IoT devices) and platforms (social media, cloud services), overwhelms investigators. Manually sifting through vast amounts of data in various formats is often impossible, leading to delays in analysis and potential loss of valuable insights.[^50, ^51]
- **Encryption and Data Deletion:** Cybercriminals frequently employ encryption to protect their data, making it difficult or impossible for investigators to access and analyze evidence without the decryption key. Furthermore, intentional data deletion by criminals using advanced techniques can make recovery exceedingly difficult, if not impossible, hindering investigations.[^51, ^52]
- **Technical Complexity for Courts:** The highly technical nature of digital evidence can be challenging for judges and juries to understand. Expert witnesses are often required to explain the significance, authenticity, and technical aspects of the evidence, adding layers of complexity and cost to legal proceedings.[^52]

5.3. Non-Legal Challenges

Beyond the purely legal and technical hurdles, a range of non-legal factors significantly impede the effective combatting of cybercrime, particularly concerning women and children.

- **Technological Advancements:** The rapid pace of technological innovation, including the emergence of artificial intelligence (AI), big data analytics, blockchain, and the Internet of Things (IoT), constantly creates new vulnerabilities that legal systems struggle to keep pace with.[^6, ^18, ^47, ^53] New forms of cybercrime, such as AI-generated deepfakes, may not be adequately covered by existing laws, leaving critical vulnerabilities in the legal system's ability to adapt.[^21]
- **Digital Literacy Gaps:** A significant challenge is the disparity in digital literacy. Many women and children, and sometimes even their parents, lack the necessary knowledge and skills to navigate the online world safely, identify threats, or understand available protective measures. This gap increases their vulnerability to various cybercrimes and hinders their

ability to effectively respond or seek help.[^54, ^55, ^56] The digital gender divide, where girls often have less access to digital services and devices, further exacerbates this issue.[^56]

- **Awareness Gaps:** There is often insufficient awareness among victims about available remedies, reporting mechanisms, and the severity of cyberviolence. Victims may be warned not to contact law enforcement or simply not know whom to contact.[^47, ^57] Similarly, law enforcement officials may be unacquainted with the phenomenon of cyberviolence and may not fully grasp its potential gravity.[^47] This lack of awareness can lead to underreporting and inadequate responses.[^58, ^59]
- **Societal Attitudes and Victim Blaming:** A pervasive non-legal challenge is the societal tendency to blame victims of cybercrime, particularly women who experience non-consensual image sharing or online harassment. Victims are often perceived as promiscuous or foolish for falling prey to scams, leading to feelings of shame, embarrassment, and self-blame.[^19, ^47, ^60] This blame can deter victims from coming forward, seeking support, or pursuing legal action, further perpetuating their isolation and distress.[^19]
- **Role of Social Media Platforms:** While social media platforms are integral to modern communication, they also serve as significant vectors for cyberviolence. Challenges include inconsistent content moderation policies, slow response times to reports of harmful content, and a lack of clear guidelines or support for victims of gender-based violence.[^47] Some platforms may even have business models that inadvertently foster criminal activity, making complaints irrelevant.[^47]
- **Resource and Expertise Shortages:** Many law enforcement agencies lack the specialized training, technical expertise, and financial resources necessary to effectively investigate and prosecute complex cybercrimes. This includes a shortage of cybersecurity experts and advanced forensic tools, hindering their ability to keep pace with evolving threats.[^47]

The confluence of these challenges reveals a fundamental asymmetry in the digital criminal landscape. Cybercriminals leverage technological advantages such as anonymity, global reach, and rapid innovation to their benefit, while legal and enforcement systems often struggle with traditional territorial boundaries, resource limitations, and a slower pace of adaptation. This creates a significant imbalance, making effective deterrence and prosecution difficult.

Furthermore, the intersection of human behavior (e.g., lack of awareness, digital literacy gaps, and ingrained societal norms) and rapid technological advancements (e.g., the development of AI and deepfakes) creates complex vulnerabilities that cannot be

resolved by technical solutions alone. The human-technology interface emerges as a critical point of exploitation. Addressing these challenges requires a holistic approach that integrates legal reforms, technological safeguards, and comprehensive social and educational interventions to build resilience and empower vulnerable populations.

6. Preventative Measures and Best Practices

Addressing the multifaceted challenges posed by cybercrimes against women and children requires a comprehensive, multi-layered approach involving individuals, families, educational institutions, governments, and the technology sector.

6.1. Individual and Family-Level Strategies

Empowering individuals and families with knowledge and tools is a foundational step in digital safety.

- **Parental Controls and Supervision:** Parental controls are software tools that allow parents to monitor, filter, limit, and block what their child sees and does online. These tools can filter adult or sexual content, manage communication, set time limits, and provide reports on online activity.[^61, ^62] While valuable, it is crucial to understand their limitations and use them in combination with other protective strategies, as children may find ways to bypass them as they get older.[^16, ^61] Keeping devices in supervised areas of the home, especially for younger children, is also advisable.[^16]
- **Open Communication and Digital Literacy:** Fostering open and continuous dialogue between parents and children about online activities is paramount. Parents should ask about their child's online experiences, who they are interacting with, and any issues they might face, reassuring them that they can always come forward without fear of punishment.[^16, ^63] Educating children about cyber safety involves explaining age limits for sites, discussing what is real versus fake online, teaching them to create strong, complex passwords, and emphasizing the importance of never clicking suspicious links or attachments.[^63]
- **Protecting Personal Information:** Children should be taught the critical importance of keeping private information confidential, including their address, phone number, full name, school, and date of birth. They should be warned against giving away personal information in usernames or at someone's request, and advised not to trust strangers online.[^63]
- **Building Resilience:** Equipping children with the ability to cope with and respond to negative online experiences is vital. This includes teaching them ways to deal with worrying or frightening online material, such as immediately telling a trusted adult, blocking and reporting online bullies,

and understanding how to adjust privacy settings.[^16] Creating a family tech agreement can also help establish clear rules and balance screen time with other activities in a constructive way.[^16, ^61]

6.2. Educational Initiatives and Awareness Campaigns

Systematic educational efforts and widespread awareness campaigns are crucial for building a more cyber-resilient society.

- **School-Based Programs:** Integrating cyber safety and digital literacy into school curricula is essential. Programs should educate students about online risks, responsible digital citizenship, and potential career paths in cybersecurity.[^17, ^38, ^64] Training for teachers is equally important to equip them with the knowledge and skills to address cybercrimes involving children, gather digital evidence, and identify/report online violence.[^38] Initiatives like UNICEF's support for digital literacy training for school directors and teachers in Ghana exemplify this.[^38]
- **Public Awareness Campaigns:** Governments and NGOs should conduct extensive public awareness campaigns using various mediums such as social media, radio, SMS, and publications. These campaigns aim to disseminate messages on cybercrime prevention, alert citizens to new modus operandi, and provide guidance on reporting incidents.[^42, ^43, ^44] Examples include India's I4C social media accounts (@CyberDost), radio campaigns, and handbooks for adolescents.[^42, ^44]
- **Targeted Training:** Specialized training programs are vital for law enforcement personnel, public prosecutors, and judicial officers to enhance their capacity in cybercrime awareness, investigation, and forensics. Platforms like India's CyTrain Portal offer online courses on critical aspects of cybercrime investigation and prosecution.[^38, ^42, ^43, ^44] UNICEF also supports training for professionals in child protection, justice, and health sectors to better understand children's digital experiences.[^38]

6.3. Policy and Governance Recommendations

Effective governance and policy frameworks are essential to create a safer digital environment and ensure accountability.

- **Strengthening Legal Frameworks:** National laws must be regularly updated to keep pace with the rapid evolution of technology. This includes expanding the definitions of cybercrime to cover emerging threats (e.g., AI deepfakes), ensuring robust and consistent legal standards for digital evidence, and addressing loopholes.[^47]
- **International Cooperation:** Given the borderless nature of cybercrime, strengthened international cooperation is indispensable. This involves

harmonizing legal definitions, establishing efficient mutual legal assistance (MLA) mechanisms, and fostering real-time information sharing among law enforcement agencies globally. The Budapest Convention's provisions for expedited preservation and disclosure of electronic evidence across borders are critical here.[^3, ^12, ^37, ^40, ^47]

- **Gender-Sensitive Approaches:** Policies and moderation procedures must incorporate a gender-sensitive approach, explicitly acknowledging gender-related and intersectional cyberviolence vulnerabilities. This includes referring to international human rights treaties on gender-based violence (e.g., Istanbul Convention) and collecting sex-disaggregated data for incidents to accurately measure and address cyber violence against women and girls.[^6]
- **Accountability of Tech Platforms:** Technology companies must be held accountable for ensuring user safety. This requires them to adopt "safety by design" principles, proactively identify and remove harmful content (e.g., child sexual abuse material), invest significantly in human content moderation, and allocate sufficient financial and non-financial resources to ensure the safety of women and children on their platforms.[^8, ^58, ^65] Clear, user-friendly reporting and response mechanisms for cyber violence incidents are also vital.[^6]
- **Public-Private Partnerships:** Collaborative efforts between governments, law enforcement, the private sector (tech companies, cybersecurity firms), and civil society organizations are crucial. These partnerships can facilitate information sharing, develop innovative solutions, and strengthen collective responses to cybercrime.[^12, ^40]
- **Addressing Digital Divide:** Initiatives to bridge the digital gender divide and improve access to technology and digital literacy for marginalized communities are essential. Ensuring equal access to digital skills training empowers women and girls to participate safely and fully in the digital economy and society.[^54, ^55]

The complexity and rapid evolution of cybercrime necessitate a multi-layered defense strategy. No single solution is sufficient; effective protection requires coordinated efforts across individual, family, community, and governmental levels, integrating technical, legal, and social strategies. This comprehensive approach acknowledges that digital safety is a shared responsibility.

Furthermore, the dynamic nature of cybercrime, particularly with the increasing role of AI in both perpetrating and combating crime, demands a fundamental shift from reactive legal and enforcement responses to proactive, anticipatory policy-making and technological solutions. This means continuously monitoring

emerging threats, investing in cutting-edge research, and developing adaptive legal frameworks that can anticipate and address future forms of digital harm, rather than merely reacting to past incidents. This proactive adaptation is critical to staying ahead of cybercriminals and truly safeguarding vulnerable populations in the digital age.

7. Conclusions

The analysis presented underscores that cybercrimes against women and children represent a rapidly escalating global threat with profound and lasting psychological, social, and financial consequences. These digital harms are not isolated incidents but often amplify and extend existing gender-based inequalities and vulnerabilities, affecting millions of individuals worldwide. While international conventions like the Budapest and Istanbul Conventions, and national laws such as India's IT Act and POCSO Act, provide foundational legal frameworks, their effectiveness is frequently challenged by the borderless nature of cybercrime, the anonymity of perpetrators, difficulties in digital evidence collection, and the rapid pace of technological advancements.

Furthermore, non-legal factors such as digital literacy gaps, insufficient awareness among victims and law enforcement, and pervasive societal attitudes that can lead to victim blaming, significantly impede the pursuit of justice and effective protection. The inherent asymmetry between agile, globally networked cybercriminals and often reactive, territorially bound legal and enforcement systems highlights a critical need for systemic transformation.

To foster a safer digital environment for women and children, a comprehensive, multi-stakeholder, and adaptive approach is imperative. This includes continuously strengthening and harmonizing legal frameworks globally, enhancing international cooperation for cross-border enforcement, and holding technology platforms accountable for implementing "safety by design" principles. Equally crucial are widespread educational initiatives and awareness campaigns to empower individuals with digital literacy and resilience, alongside a societal shift away from victim-blaming attitudes. Ultimately, safeguarding women and children in the digital age is a human rights imperative, demanding sustained and coordinated efforts across all sectors to ensure their full and safe participation in an increasingly interconnected world.

References

[^1]: Proofpoint. “Cybercrime.” *Proofpoint*. August 14, 2025. https://www.proofpoint.com/us/threat-reference/cyber-crime [^2]: Cybertalents. “What is Cyber Crime? Types, Examples, and Prevention.” *Cybertalents.com*. August 14, 2025. https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention [^3]: Kumar, C. Raj. “Cybercrime and the Law: Challenges in Prosecuting Digital Offenses.” *Indian Journal of Law*. September 2024. https://www.researchgate.net/publication/384390350_Cybercrime_and_the_Law_Challenges_in_Prosecuting_Digital_Offenses [^4]: U.S. Government Accountability Office. “The U.S. Is Less Prepared to Fight Cybercrime Than It Could Be.” *GAO Blog*. August 29, 2023. https://www.gao.gov/blog/u.s.-less-prepared-fight-cybercrime-it-could-be [^5]: ICRC. “Online violence: real life impacts on women and girls in humanitarian settings.” *Blogs.ICRC.org*. January 4, 2024. https://blogs.icrc.org/law-and-policy/2024/01/04/online-violence-real-life-impacts-women-girls-humanitarian-settings/ [^6]: European Institute for Gender Equality. “Cyber violence against women.” *EIGE*. May 14, 2024. https://eige.europa.eu/gender-based-violence/cyber-violence-against-women?language_content_entity=en [^7]: Nesslany, Léa. “Cybercrime and psychological risks.” *Cn2r.fr*. November 6, 2024. https://cn2r.fr/en/article-scientifique-cyberpedocriminalite/ [^8]: The Patrick J. McGovern Foundation. “Violence-free digital spaces are a right. For women and girls, that right is rarely guaranteed.” *Medium*. July 21, 2025. https://medium.com/@PatrickJMcGovern_Foundation/violence-free-digital-spaces-are-a-right-for-women-and-girls-that-right-is-rarely-guaranteed-1eec654fc872 [^9]: Norwich University. “5 Types of Cyber Crime & How Cybersecurity Professionals Prevent Attacks.” *Norwich.edu*. August 14, 2025. https://online.norwich.edu/online/about/resource-library/5-types-cyber-crime-how-cybersecurity-professionals-prevent-attacks [^10]: Cybertalents. “What is Cyber Crime? Types, Examples, and Prevention.” *Cybertalents.com*. August 14, 2025. https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention [^11]: Franklin, A. “Why did she send it in the first place? Victim blame in the context of ‘revenge porn’.” *PMC*. September 2016. https://pmc.ncbi.nlm.nih.gov/articles/PMC7534260/ [^12]:

INTERPOL. “Cybercrime.” *Interpol.int*. August 14, 2025. https://www.interpol.int/Crimes/Cybercrime [^13]: Astra. “Cyber Crime Statistics.” *GetAstra.com*. June 20, 2025. https://www.getastra.com/blog/security-audit/cyber-crime-statistics/ [^14]: AAG-IT. “The Latest Cyber Crime Statistics.” *AAG-IT.com*. July 2025. https://aag-it.com/the-latest-cyber-crime-statistics/ [^15]: INTERPOL. “Our analysis reports.” *Interpol.int*. August 14, 2025. https://www.interpol.int/How-we-work/Criminal-intelligence-analysis/Our-analysis-reports [^16]: eSafety Commissioner. “Online safety basics.” *eSafety.gov.au*. September 3, 2024. https://www.esafety.gov.au/parents/issues-and-advice/online-safety-basics [^17]: National Cybersecurity Alliance. “Career and Education – External Resources.” *StaySafeOnline.org*. August 14, 2025. https://www.staysafeonline.org/resources/career-and-education/external-resources [^18]: PMC. “Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations.” *PMC*. July 25, 2023. https://pmc.ncbi.nlm.nih.gov/articles/PMC10422504/ [^19]: Journal of the American Academy of Psychiatry and the Law. “Revenge Pornography: Mental Health Implications and Related Legislation.” *JAAPL.org*. September 2016. https://jaapl.org/content/44/3/359 [^20]: National Organization for Women & Incogni. “Online abuse against women in the US.” *NOW.org*. March 5, 2025. https://now.org/wp-content/uploads/2025/03/NOWxIncogni_Online-abuse-survey.pdf [^21]: National Organization for Women & Incogni. “Online abuse against women in the US.” *NOW.org*. March 5, 2025. https://now.org/wp-content/uploads/2025/03/NOWxIncogni_Online-abuse-survey.pdf [^22]: DL Press. “Psychological Effects of Cybercrime on Minorities: Short-Term and Long-Term Impacts.” *Publications.DLPress.org*. August 14, 2025. https://publications.dlpress.org/index.php/jesss/article/download/3/2/5 [^23]: UN Women. “FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women.” *UNWomen.org*. February 10, 2025. https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women [^24]: UN Women. “Accelerating efforts to tackle online and technology facilitated violence

against women and girls (VAWG).” *UNWomen.org*. October 2022. https://www.unwomen.org/sites/default/files/2022-10/Accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls-en_0.pdf [^25]: UN Women. “Accelerating efforts to tackle online and technology-facilitated violence against women and girls.” *UNWomen.org*. 2022. https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls [^26]: McLean Hospital. “Understanding the Mental Health Toll of Bullying on Young People.” *McLeanHospital.org*. May 5, 2025. https://www.mcleanhospital.org/essential/bullying-kids-teens [^27]: Australian Human Rights Commission. “Cyberbullying, Human rights and bystanders.” *HumanRights.gov.au*. August 14, 2025. https://humanrights.gov.au/our-work/childrens-rights/cyberbullying-human-rights-and-bystanders-0 [^28]: Singh, Shivani. “Cyber Crime against school children: Challenges & Solutions.” *ResearchGate*. January 2020. https://www.researchgate.net/publication/384369850_Cyber_Crime_against_school_children_Challenges_Solutions [^29]: National Center for Missing & Exploited Children. “CyberTipline Data.” *MissingKids.org*. 2024. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata [^30]: Georgia State University News. “Study Estimates 1 in 12 Children Subjected to Online Sexual Exploitation or Abuse.” *News.GSU.edu*. January 22, 2025. https://news.gsu.edu/2025/01/22/study-estimates-1-in-12-children-subjected-to-online-sexual-exploitation-or-abuse/ [^31]: United Nations. “Child and Youth Safety Online.” *UN.org*. August 14, 2025. https://www.un.org/en/global-issues/child-and-youth-safety-online [^32]: The Hindu. “HC warns of severe action for cybercrimes targeting children.” *TheHindu.com*. August 1, 2025. https://www.thehindu.com/news/cities/Delhi/hc-warns-of-severe-action-for-cybercrimes-targeting-children/article69884581.ece [^33]: UNODC. “United Nations Convention against Cybercrime.” *UNODC.org*. August 14, 2025. https://www.unodc.org/unodc/cybercrime/convention/home.html [^34]: Council of Europe. “Protecting women and girls from violence in the digital age (2021).” *edoc.coe.int*. December 2021. https://rm.coe.int/the-relevance-of-the-ic-and-the-budapest-convention-on-cybercrime-in-a/1680a5eba3 [^35]: States Assembly. “Research – Briefing Paper on Council of

Europe Convention on Cybercrime – 31 October 2018." *StatesAssembly.je*. October 31, 2018. https://statesassembly.je/getmedia/baff60aa-468b-4914-8420-d3fc58f1698d/Research%20-%20Briefing%20Paper%20on%20Council%20of%20Europe%20Convention%20on%20Cybercrime%20-%2031%20October%202018.pdf [^36]: Council of Europe. "Protecting women and girls from violence in the digital age (2021)." *edoc.coe.int*. December 2021. https://edoc.coe.int/en/violence-against-women/10686-protecting-women-and-girls-from-violence-in-the-digital-age.html [^37]: UNODC. "Global Programme to end Violence Against Children_Legal Framework." *UNODC.org*. August 14, 2025. https://www.unodc.org/unodc/justice-and-prison-reform/global-programme-to-end-violence-against-children_legal-framework.html [^38]: UNICEF. "Tackling online violence against children." *UNICEF.org*. August 14, 2025. https://www.unicef.org/media/150116/file/Tackling%20Online%20Violence%20Against%20Children.pdf [^39]: Europol. "Common Challenges in Cybercrime." *Europol.europa.eu*. August 14, 2025. https://www.europol.europa.eu/publications-events/publications/common-challenges-in-cybercrime [^40]: INTERPOL. "Cybercrime Collaboration Services." *Interpol.int*. August 14, 2025. https://www.interpol.int/Crimes/Cybercrime/Cybercrime-Collaboration-Services [^41]: National Commission for Women. "Copy of CYBER LAW GUIDE DRAFT MANUSCRIPT NATIONAL COMMISSION FOR WOMEN NEW DELHI." *cdn.ncw.gov.in*. May 13, 2025. https://cdn.ncw.gov.in/wp-content/uploads/2025/05/CyberSaheli.pdf [^42]: Ministry of Home Affairs. "CYBER CRIME PREVENTION AGAINST WOMEN AND CHILDREN (CCPWC) SCHEME." *PIB.gov.in*. March 11, 2025. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2110359 [^43]: Ministry of Women and Child Development. "Measures To Ensure Safety And Security Of Women And Children On Online Platforms." *PIB.gov.in*. March 23, 2022. https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1808686 [^44]: Ministry of Home Affairs. "CYBERCRIME AGAINST WOMEN." *MHA.gov.in*. March 18, 2025. https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS18032025/2944.pdf [^45]: Seth Associates. "Explained:

Everything You Need To Know About Protecting Kids From Cyber Crimes (Youth ki Awaaz).” *SethAssociates.com*. August 14, 2025. https://www.sethassociates.com/explained-everything-need-know-protecting-kids-cyber-crimes-youth-ki-awaaz.html [^46]: ResearchGate. “(PDF) CYBERCRIME AGAINST WOMEN IT’S EVOLUTION AND EFFECTS ON PERSONAL LIFE.” *ResearchGate.net*. August 8, 2025. https://www.researchgate.net/publication/389675085_CYBERCRIME_AGAINST_WOMEN_IT’S_EVOLUTION_AND_EFFECTS_ON_PERSONAL_LIFE [^47]: Leppard Law. “Examining Jurisdictional Challenges in Cyber Threat Investigations in the US.” *LeppardLaw.com*. August 14, 2025. https://leppardlaw.com/federal/computer-crimes/examining-jurisdictional-challenges-in-cyber-threat-investigations-in-the-us/ [^48]: Council of Europe. “Challenges to the investigation and prosecution.” *coe.int*. August 14, 2025. https://www.coe.int/en/web/cyberviolence/challenges-to-the-investigation-and-prosecution [^49]: Kailash Satyarthi Children’s Foundation. “Cyber Crime Report.cdr.” *Satyarthi.org.in*. April 2023. http://satyarthi.org.in/wp-content/uploads/2023/04/Cyber-Crime-Report_F.pdf [^50]: Vidizmo. “8 Challenges in Digital Evidence Handling and Effective Solutions.” *Vidizmo.ai*. July 25, 2025. https://vidizmo.ai/blog/handling-digital-evidence [^51]: SciELO México. “Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations.” *SciELO.org.mx*. May 9, 2025. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-05782024000100023 [^52]: Leppard Law. “Digital Evidence Challenges in Federal Cybercrime Trials.” *Federal-Criminal.com*. August 14, 2025. https://federal-criminal.com/computer-crimes/digital-evidence-challenges-in-federal-cybercrime-trials/ [^53]: MDPI. “Cybercrime Resilience in the Era of Advanced Technologies: Evidence from the Financial Sector of a Developing Country.” *MDPI.com*. January 27, 2025. https://www.mdpi.com/2073-431X/14/2/38 [^54]: World Bank. “Publication: What Works to Advance Women’s Digital Literacy?: A Review of Good Practices and Programs.” *OpenKnowledge.WorldBank.org*. August 14, 2025. https://openknowledge.worldbank.org/entities/publication/6c1c1818-1085-4036-8a4d-c64c0dbb7f40 [^55]: Plan International. “Bridging the digital gender divide.” *Plan-International.org*. August 14, 2025. https://plan-

international.org/quality-education/bridging-the-digital-divide/ [^56]: eSafety Commissioner. “Mind the Gap – Parental awareness of children’s exposure to risks online.” *eSafety.gov.au*. February 2022. https://www.esafety.gov.au/sites/default/files/2022-02/Mind%20the%20Gap%20%20-%20Parental%20awareness%20of%20children%27s%20exposure%20to%20risks%20online%20-%20FINAL.pdf [^57]: GOV.UK. “Experiences of victims of fraud and cyber crime.” *GOV.UK*. January 14, 2025. https://www.gov.uk/government/publications/experiences-of-victims-of-fraud-and-cyber-crime/experiences-of-victims-of-fraud-and-cyber-crime [^58]: eSafety Commissioner. “Parental controls.” *eSafety.gov.au*. August 8, 2025. https://www.esafety.gov.au/parents/issues-and-advice/parental-controls [^59]: San Diego County Office of Education. “Ed Tech Team Launches Virtual Parent Training Series on Online Safety.” *SDCOE.net*. August 5, 2025. https://www.sdcoe.net/about-sdcoe/news/post/~board/news/post/ed-tech-team-launches-virtual-parent-training-series [^60]: Hindustan Times. “Push to protect children online faces basic challenges: Experts.” *HindustanTimes.com*. January 5, 2025. https://www.hindustantimes.com/india-news/push-to-protect-children-online-faces-basic-challenges-experts-101736015737739.html [^61]: eSafety Commissioner. “Parental controls.” *eSafety.gov.au*. August 8, 2025. https://www.esafety.gov.au/parents/issues-and-advice/parental-controls [^62]: New York City Department of Education. “Tools for Keeping Children Safe Online.” *Schools.nyc.gov*. August 14, 2025. https://www.schools.nyc.gov/learning/digital-learning/applications-and-platforms/tools-for-keeping-children-safe-online [^63]: New York City Department of Education. “Tools for Keeping Children Safe Online.” *Schools.nyc.gov*. August 14, 2025. https://www.schools.nyc.gov/learning/digital-learning/applications-and-platforms/tools-for-keeping-children-safe-online [^64]: Gen Digital. “Bringing online safety education to 1 million people in India.” *GenDigital.com*. May 18, 2022. https://www.gendigital.com/blog/archive/cyber-safety-india-0 [^65]: WeProtect Global Alliance. “WeProtect Global Alliance.” *WeProtect.org*. August 14, 2025. https://www.weprotect.org/ [^66]: UNICEF. “Childhood in

a Digital World." *UNICEF.org*. June 2025. https://www.unicef.org/innocenti/reports/childhood-digital-world