Welens

EDUCATIONAL PRACTICES THROUGH A GENDER LENS

SEXUAL EXPLOITATION & VIOLENCE TOOLKIT

MODULE 4
Digital Technologies and Gender-Based Violence

Co-funded by the European Union

Project number 2023-1-FR01-KA220-ADU-000165625

While the terminology used in the English, Spanish, Estonian, Russian and French version of this toolkit refer to Prostitution as lacking of agency and harmful in any of its forms, this Toolkit in its Italian and Greek versions have been developed in the recognition of an ongoing debate about prostitution, sex work and sexual exploitation which better reflect the official position of CESIE ETS and that of Greece's legal framework and of the Center for security Studies' researchers.

Specifically, in the Italian and Greek toolkit, the term "sexual exploitation in prostitution" is used, which refers to a form of sexual violence that involves a person profiting from the use of another person's body in a sexual manner, whether financially or through other means and which is nonconsensual and harmful.

Both CESIE ETS and researchers from the Center for Security Studies recognise the importance of distinguishing what is mentioned above from sex work, which is understood as the consensual provision of sexual services between adults. This takes many forms, varies between and within countries and communities, and is undertaken for money, goods, or rewards, recognising the agency of individuals engaged.

As a result, "prostitution", even if valid in legal frameworks, will not be used as it is an umbrella term which does not take into consideration the above-mentioned nuances.

Contents

GLOSSARY

Algorithmic Discrimination

Automated systems that produce biased or unfair outcomes, often disadvantaging people based on race, gender, age, or class. Bias comes from flawed data, design, or wider structural inequalities.

Information and Communication Technologies (ICT)

Tools and platforms for storing, sharing, and accessing information, such as phones, internet services, and apps.

Gender-Based Violence (GBV)

Harmful acts directed at people because of their gender, including physical, sexual, psychological, and economic abuse.

Technology-Facilitated Gender-Based Violence (TFGBV)

Any form of GBV carried out, enabled, or worsened through digital technologies like social media or messaging apps.

Trolling

Posting offensive or provocative comments online to upset or silence others.

Human Trafficking

Exploiting people through force, fraud, or coercion for labour, sexual exploitation, or other purposes, often using online platforms.

Online Exploitation

Abuse or manipulation through the internet, including blackmail, grooming, trafficking, and sexual exploitation.

Online Harassment

Aggressive or threatening behaviour online, such as persistent messages, name-calling, threats, sexual harassment, or coordinated attacks.

Digital Footprint

The record left behind by people's online activity.

- **Active Digital Footprint** – Information users create directly, like posts, likes, or uploads.
- **Passive Digital Footprint** – Information collected automatically, such as browsing history, cookies, or location data.

Cyberstalking

Ongoing digital surveillance or harassment that causes fear and distress.

Cyberbullying

Repeated online humiliation or harassment targeting an individual.

Cybermob Attacks (Dogpiling)

Large groups harassing one person online, often after a single post or opinion.

Catfishing

Using fake identities online to deceive, manipulate, or exploit others.

Doxxing

Publishing private or identifying details about someone online without consent.

Deepfake Pornography / Deepfake Abuse

AI-generated sexual or fake videos and images that depict someone without their consent.

Debt Bondage

Exploiting people by tying them to debts they cannot repay, forcing them into labour or servitude.

Digital Literacy

The skills to safely and critically use digital tools, understand risks, and protect privacy.

Disinformation

False information created and spread deliberately to mislead or manipulate.

Survivor-Centred Design

Technology design that prioritises the safety and needs of people who have experienced violence.

Intersectionality

Understanding how overlapping identities (gender, race, class, migration status, etc.) shape experiences of discrimination and privilege.

CEDAW (Convention on the Elimination of All Forms of Discrimination Against Women)

A UN treaty requiring states to eliminate discrimination against women, including digital violence.

Istanbul Convention

A Council of Europe treaty against violence towards women and domestic violence, recognising online abuse like stalking.

Image-Based Abuse / Non-Consensual Image Sharing (NCII)

Sharing intimate or sexual images without consent, often called “revenge porn.”

Incels (Involuntary Celibates)

Online groups of men expressing resentment or violence towards women due to perceived sexual rejection.

Misinformation

False information spread without intent to mislead.

Budapest Convention

The first international treaty on cybercrime, setting legal standards for digital offences.

Digital Services Act (DSA)

An EU regulation requiring online platforms to remove illegal content and protect users.

Digital Inclusion

Ensuring all people, especially marginalised groups, can access and use digital technologies.

General Data Protection Regulation (GDPR)

EU law protecting personal data and privacy online.

Geotagging

Attaching location data to media like photos or videos.

Gendered Disinformation

False or misleading content that uses sexist narratives or stereotypes to discredit women and gender minorities.

Sextortion

Blackmail where sexual content is threatened to be released unless demands are met.

Hacking and Account Takeovers

Gaining unauthorised access to accounts to steal data, impersonate, or lock people out.

Hate Speech and Misogynistic Memes

Online content spreading sexist or violent ideas.

Dynamic Blocking

A Greek legal mechanism to block access to websites with illegal or pirated content.

Grooming

Building trust with minors or vulnerable individuals online for exploitation or abuse.

Right to Be Forgotten

The legal right to have personal data deleted when it is no longer necessary, accurate, or lawfully kept.

INTRODUCTION

1. Introduction: Digital Technologies and Gender-Based Violence: Combatants and Enablers

The advent of digital technologies has radically reconfigured how individuals interact, access information, and mobilise social change. But this transformation has not been without complexity, particularly for women and girls navigating the digital sphere. Digital Technologies, also known as Information and Communication Technologies (ICT), hold profound potential to empower survivors of gender-based violence (GBV), enabling access to support networks, legal protection, and avenues for collective resistance. Yet simultaneously, these same tools can be—and increasingly are—hijacked to perpetrate abuse, facilitate human trafficking, and entrench power imbalances.

This chapter aims to unpack the dual role of ICT in both enabling and combating gender-based violence and exploitation. It also interrogates the concept of the digital footprint, revealing how women's data trails online can be harnessed for safety or weaponised for control. In doing so, the text draws from global research, case studies, and policy developments to provide a comprehensive understanding of how digital ecosystems shape vulnerability and resilience.

1.1. ICT as a tool of empowerment

At its best, ICT offers transformative possibilities for addressing GBV. Survivors now have access to digital helplines, crisis text services, and mobile applications that facilitate discreet communication with support providers. These tools bypass barriers such as geographic isolation, social stigma, and fear of retaliation, especially in contexts where accessing physical services may be dangerous or impossible.

Social media platforms also play an increasingly important role in collective advocacy. Movements like #MeToo, #SayHerName, and #NiUnaMenos demonstrate how digital spaces have become arenas for storytelling, solidarity, and mobilisation. Such campaigns not only raise awareness but also influence policy reform and cultural shifts. In regions where mainstream institutions neglect or dismiss women's safety concerns, ICT becomes a gateway to visibility and justice.

Digital inclusion initiatives further amplify these effects. For example, women in remote or underserved areas gain access to tele-legal support, psychosocial counselling, and e-learning programs that challenge the isolation historically used to silence or disempower them. Interactive platforms also allow survivors to document experiences, track incidents of abuse, and connect anonymously with peer support communities. Research confirms that digital literacy correlates with increased help-seeking behaviour and better safety outcomes.

1.2. ICT as a mechanism of control and abuse

Despite the promise of technological progress, digital spaces have also become fertile ground for misogyny and exploitation. **Technology-facilitated gender-based violence (TFGBV)** encompasses a range of abusive practices: cyberstalking, online harassment, non-consensual image sharing ("revenge porn"), impersonation, and threats of physical harm[^5]. These violations are amplified by scale and permanence—content circulated online can reach thousands instantly and remain accessible indefinitely. **The internet is forever;** once shared, harmful material can be copied, archived, or re-uploaded, making it nearly impossible for survivors to remove it fully.

Moreover, perpetrators are increasingly leveraging encryption tools, anonymous browsing, and the dark web to escape accountability. In cases of human trafficking, digital platforms are used to recruit, groom, and control victims without physical contact. Traffickers advertise services on social media, use geolocation data to track movement, and exploit dating apps to lure women into false relationships that later turn exploitative.

The psychological toll of TFGBV should not be underestimated. Victims often report feelings of hypervigilance, shame, and powerlessness, compounded by the difficulty of removing harmful content or identifying abusers. Law enforcement agencies frequently lack the digital capacity or jurisdictional authority to intervene, leaving survivors in a state of perpetual exposure. This persistent exposure can result in re-traumatisation, as survivors are forced to relive the original harm each time the abusive content resurfaces online.

1.3. The digital footprint: a map of vulnerability

Central to understanding online exploitation is the concept of the digital footprint—the trail of data generated through an individual's interaction with digital platforms. This includes active footprints such as social media posts, online purchases, and messages, as well as passive footprints, including metadata, location tracking, cookies, and browsing history.

While digital footprints can assist in gathering forensic evidence against perpetrators, they also present significant risks. For women fleeing abusive relationships or coercive environments, their digital presence can be used to locate and harass them. Geotagged photos, predictive algorithms, and cross-platform data harvesting mean survivors are not only vulnerable to known abusers but also to targeted marketing, surveillance, and even algorithmic discrimination.

Young women and girls face particular challenges. Studies show that adolescent girls tend to have lower control over digital settings, are more likely to borrow devices, and often lack access to comprehensive digital education. Moreover, girls from marginalised backgrounds—such as migrants, LGBTQ+ youth, or those experiencing poverty—encounter compounded risks due to systemic exclusion and limited digital agency.

TYPES OF ONLINE GENDER-BASED VIOLENCE

2. Types of online gender-based violence

Technology-facilitated gender-based violence, or online gender-based violence (GBV), is a form of systemic abuse that uses digital technologies to target, silence, and control individuals based on their gender. It disproportionately affects women and girls, reinforcing power imbalances and perpetuating offline discrimination. Online GBV is not accidental or isolated — it is part of a wider continuum of violence that spans both physical and virtual spaces. Its impacts are real, long-lasting, and often devastating.

This type of violence shows up in many ways. **Online harassment**, **cyberbullying**, and **cyberstalking** are among the most common, ranging from constant unwanted messages and threats to invasive monitoring. **Trolling** and **cybermob attacks (dogpiling)** involve hostile comments or large groups overwhelming a person with abuse, often after they express an opinion online. Technical intrusions such as **hacking**, **identity theft**, and **doxxing** expose people to further harm by stealing personal data, impersonating them, or publishing private information.

Image-based abuse is another powerful weapon. This includes the non-consensual sharing of intimate photos or videos, **sextortion**, or the use of manipulated material such as **deepfakes**. Deception also plays a role: **catfishing** uses false identities to mislead and exploit others, while **grooming** involves building trust with minors or vulnerable people to prepare them for sexual abuse. Alongside these tactics, **hate speech** and **misogynistic memes** circulate widely, reinforcing stereotypes and making abuse appear acceptable.

Each of these forms is described in more detail in the glossary, but together they illustrate how online GBV uses digital spaces to extend and intensify gendered violence.

These forms of violence can overlap and often have severe psychological, social, and even economic consequences for victims.

What's the difference between a bully and a hater online? A bully usually targets a specific person repeatedly, often trying to dominate, intimidate, or humiliate them over time. A hater, on the other hand, may post harmful, hostile, or toxic comments without a personal connection or ongoing focus, often driven by prejudice or trolling culture rather than a personal vendetta. While both are harmful, bullying tends to be more persistent and personal.

2.1. The impact of social media

Digital spaces are where all public life happens. Social media platforms have become central to how people connect, express themselves, and access information. However, they have also created new environments where gender-based violence (GBV) can occur, often with a broad reach and devastating impact. Online GBV is not only a reflection of offline inequality but also a mechanism that reinforces it through technology.

- **Amplification of abuse**

Social media can rapidly amplify harassment, threats, and shaming. A single abusive comment can be reshared, liked, or piled onto by others, turning a personal attack into a viral event.

- **Anonymity and lack of accountability**

While anonymity can protect vulnerable users, it also allows perpetrators to harass others with little fear of consequences. Fake profiles and weak moderation systems contribute to a culture where threats and abuse are rarely addressed effectively.

- **Normalisation of harmful content**

Sexist jokes, rape culture, and misogynistic memes often circulate widely and are dismissed as "just humour" or "freedom of speech." This normalises violence, reinforces gender stereotypes, and discourages survivors from speaking out.

    - **Incel communities**: Online subcultures such as incels (involuntary celibates) are a key driver of misogynistic content and gendered hate speech. Incel forums and social media spaces normalise hostility towards women, promote harmful stereotypes, and sometimes glorify sexual violence.

- **Surveillance and control**

Social media can be used to monitor, stalk, or control someone's behaviour, especially in abusive relationships. Features like geotagging, "seen" messages, or tagging in photos can be weaponised to track and intimidate.

- **Silencing, self-censorship and fear of speaking up**

Faced with constant harassment, many women and marginalised individuals limit what they share, leave platforms, or avoid participating in public discourse. Others choose not to speak up about experiences of technology-facilitated GBV at all, fearing bullying, humiliation, victim-blaming, or not being believed. This leads to the silencing of critical voices and perspectives, and reinforces the perception that online spaces are unsafe for women.

- **Spread of misinformation and gendered disinformation**

Social media is a powerful tool for spreading false information, including harmful gender-based stereotypes or targeted disinformation campaigns aimed at women activists, journalists, or politicians to undermine their credibility and safety.

2.2. The dual nature of anonymity

Anonymity plays a complex and often controversial role in the context of online gender-based violence (GBV). Its effects are both enabling and protective, depending on the perspective and context.

How anonymity enables perpetrators

- Reduced Accountability**:** The ability to hide one's identity online can embolden individuals to engage in abusive behaviours, such as harassment, threats, and stalking, without fear of real-world consequences.
- Escalation of Abuse**:** Anonymity can facilitate more aggressive or persistent forms of abuse, as perpetrators feel shielded from detection and punishment.
- Difficulty in Enforcement: Law enforcement and platform moderators often face challenges in identifying and prosecuting offenders when their identities are concealed, making it harder to hold perpetrators accountable.

How anonymity protects victims

- Safety for Survivors**:** For victims and survivors of GBV, anonymity can be crucial for seeking support, sharing experiences, or participating in advocacy without risking retaliation or further harm.
- Privacy for Vulnerable Groups**:** Women, activists, and those in oppressive environments may rely on anonymous identities to express themselves safely and access resources.
- Empowerment**:** Anonymity enables some users to participate in online spaces they might otherwise avoid due to fear of being targeted or experiencing discrimination.

CROSS-SECTORAL AND STATE SYNERGIES IN ADDRESSING GENDER-BASED VIOLENCE

3. Cross-Sectoral and State Synergies in Addressing Gender-Based Violence

Gender-based violence (GBV) is not just a personal, nor an isolated trauma — it is a deeply entrenched, continuous global crisis that echoes across - and impacts - every layer of society. Whether it is the strain on healthcare systems, the ripple effects through education systems, or the cost for economic growth, GBV leaves no sector untouched. Even more so, when its online forms are penetrating the lives of women wherever they may reside, across nations and continents. Hence, tackling online GBV requires more than individual country efforts; it calls for genuine, sustained collaboration among governments, communities, and institutions, driven by shared accountability and mutual trust.

Most states now recognise GBV as a violation of human rights. Legal instruments, such as the Istanbul Convention and CEDAW, have prompted governments to adopt national laws and strategies. But having a framework is not enough. Implementation is where many countries fall short. Some countries still lack survivor-centred approaches or fail to allocate proper funding. Others have laws on paper (possibly to abide by international or regional frameworks and initiatives), but lack adequate enforcement mechanisms.

Cross-sector collaboration is vital, as no single sector can address online GBV alone. Health services, law enforcement, education, and social welfare must work together in a complementary manner to achieve effective outcomes. For example, hospitals need protocols for identifying abuse and referring survivors; police must be trained to handle cases sensitively and promptly; schools should teach consent and respect early on. When these sectors operate alone, survivors fall through the cracks. That is why integrated referral systems and joint training programs can have a tangible impact by bridging these gaps.

International Cooperation is increasingly crucial, as online violence does not respect borders, nor is it contained within the boundaries of any one country. Trafficking, online abuse, and forced migration all have cross-border dimensions. Enter international cooperation: UN bodies, regional alliances, and NGOs play a key role in sharing data, funding programs, and holding states accountable. The Sustainable Development Goals (especially SDG5) have helped align global efforts, but more needs to be done to ensure commitments are translated into action.

It is safe to conclude that the fight against online GBV is complex. It is not only about punishing perpetrators after the crime is committed—it is also about changing systems at their core. To that end, states must move beyond rhetoric. Sectors must stop working in isolation, and international actors must keep pushing for accountability.

3.1. European Union Frameworks

There are EU-wide laws and pertinent mechanisms for protecting users—especially women and minors—on online platforms, including pornographic websites, as well as for how to report and/or request content removal.

As per EU Laws on Online Platforms and Pornographic Websites, there is the Digital Services Ac (DSA) Regulation, which is fully applicable since 17 February 2024 and applies to all platforms. Especially the Very Large Online Platforms (VLOPs) such as Pornhub, Stripchat, and XVideos must:

- Conduct risk assessments not only of possible illegal content, but also specifically of gender-based violence and child safety online.
- Implement systems pertaining to age verification so as to block access from minors on sites containing pornographic content.
- Remove immediately content flagged or reported as illegal or non-consensual.
- Be transparent and accountable by undergoing independent audits.
- Be at all times subject to scrutiny for both bias and harm.

Non-compliance with any of the above-mentioned may lead to fines up to 6% of their global annual turnover or even EU-wide bans.

Further, to protect women online, the Cyberviolence Directive of 2024, which is set to be implemented by 2027, includes the criminalisation of revenge porn, cyberstalking, online sexual harassment, and non-consensual deepfakes. Also, to that end, websites must remove intimate or manipulated images that are posted online without consent. Through an EU-wide directive, victims shall gain access to justice and support services across the EU.

Reporting harmful or illegal online content may be done in various ways:

- Directly to the pertinent platforms using their DSA-compliant tools
- Through civil society groups designated explicitly by the EU to escalate the most serious cases
- National digital services coordinators (DSCs), who are bodies formed in each EU MS to oversee compliance of websites with the DSA

- For more difficult/complicated cases, complaints may be submitted directly via the EU Digital Strategy portal.

Thus, a comprehensive step-by-step visualisation of how to report an online crime is as follows:

STEP 1: Identify Content

↓

Specify the harmful or illegal content and its location (URL)

↓

STEP 2: Explain Breach

↓

Describe how the content violates the DSA or GDPR.

↓

STEP 3: Provide Details

↓

Include your relationship to the content and any supporting evidence.

↓

STEP 4: Request Removal

↓

Ask for immediate removal and a timely response.

3.2. National Frameworks

FRANCE

France has implemented a comprehensive legal framework to protect minors from exposure to pornographic and harmful content online. The country combines criminal law, digital regulation, and strict enforcement mechanisms to ensure compliance, especially following the recent EU Digital Services Act (DSA).

Legal and policy framework

- **French Penal Code (Article 227-24)** prohibits making pornographic content accessible to minors. The law applies to both physical and online distribution. Non-compliant operators risk **up to 3 years in prison and €75,000 in fines**.
- **Law No. (2024).-449** (SREN – Law to Secure and Regulate the Digital Space), enacted in **May 2024**, requires websites with pornographic content to implement **robust age verification systems**. This law applies to all sites accessible from France, including those hosted outside of France.
- **ARCOM**, the national regulatory authority, was empowered to monitor and enforce these obligations. It can issue formal warnings, impose fines, request audits, and order access restrictions or **blocking of non-compliant websites**.

  (**ARCOM** – Regulatory Authority for Audiovisual and Digital Communication)

Enforcement and age verification measures

- In **October 2024**, ARCOM released its **technical guidelines** for compliant age verification:
  - Use of **double anonymity systems**, ensuring no linkage between a user's identity and their browsing behaviour.
  - Independent **third-party verification**, separate from the platform itself.
  - **No storage of personal data** or identifiers.
- A **transitional mechanism** using temporary bank card verification was allowed until early 2025. Currently, sites must transition to full compliance by utilising certified anonymous verification systems.
- In **early 2025**, ARCOM published a list of **17 adult websites** (including Pornhub, RedTube, and others) subject to mandatory compliance. As of mid-2025, **multiple sites have been blocked or delisted** due to failure to implement proper controls, as approved by the court.

- Fines under the SREN law can reach **€150,000 or up to 2% of global annual revenue**, with escalating measures for repeat offenders.

How to report illegal content or request removal

Situation	Platform/Authority	Description
Illegal content (e.g., child sexual abuse material, grooming, terrorist content)	**PHAROS**	National online crime reporting platform operated by the Ministry of Interior. Anonymous submissions are accepted. www.internet-signalement.gouv.fr
Cyberbullying, revenge porn, unwanted exposure to adult content, sextortion	**3018 (e-Enfance Association)**	Dedicated helpline for minors and parents. Fast-track reporting to platforms like TikTok, YouTube, and Instagram. Free, confidential, available by phone, SMS, chat, or app. www.3018.fr
Personal data exposure, right to be forgotten	**CNIL** (French Data Protection Authority)	Handles GDPR-related requests for data erasure or removal from search engines. www.cnil.fr

- As of late 2024, **e-Enfance was officially designated as a "trusted flagger" by ARCOM**, meaning major platforms prioritise reports from 3018.

France's legal and institutional framework strongly prioritises **the protection of minors from online pornography and digital abuse**. New laws (SREN) impose age verification requirements and empower ARCOM to enforce them. Criminal law (Article 227-24) punishes exposure of minors to such content. Reporting systems, such as **PHAROS** (for illegal content) and **3018** (for support and fast removal), offer effective protection pathways for users. France thus combines **strict legislation, active enforcement, and user-friendly reporting mechanisms, in line with its** EU obligations under the **Digital Services Act (DSA)**.

ITALY

In Italy, there are specific regulations that govern the protection of personal data and establish mandatory security measures to be adopted. One of the main regulations in this area is the General Data Protection Regulation (GDPR), which came into force in 2018. This regulation sets out a series of principles and obligations that organisations must comply with to ensure the protection of personal data. Among the mandatory security measures provided by the GDPR is the adoption of appropriate technical and organisational measures to ensure a level of security appropriate to the risk. These measures may include the use of encryption, implementing backup procedures, and controlling access to data. In addition to the GDPR, Italy has other regulations governing the protection of personal data. For example, the Personal Data Protection Code (Legislative Decree 196/2003) establishes the security measures that organisations must adopt to protect personal data. Among these measures is the obligation to adopt suitable technical and organisational measures to ensure the security of personal data and to prevent loss, destruction, or unauthorised access (Diritto.net, 2023b).

Regarding pornography, in Italy, watching pornographic videos on the internet, that is, via streaming, is legal, as is downloading them. However, in the case of downloads, one must ensure that the content is free to use — that is, not protected by copyright — otherwise, one may incur a different penalty for copyright infringement. However, child pornography, that is, pornography involving minors, is a separate matter. In this case, although merely viewing such videos on the internet is not punishable, the possession or distribution of the material is (La Legge Per Tutti, 2015). The Italian Penal Code, in Article 600-bis, defines child pornography as the production, possession, distribution, and transfer of pornographic material involving minors under the age of 18. This offence is considered particularly serious and is actively prosecuted by law enforcement authorities. To effectively combat child pornography and online crimes against minors, several legislative measures have been adopted. Among these, Law No. 38/2006 introduced the offence of child grooming via the internet, penalising anyone who approaches a minor with the intent to commit sexual crimes (Diritto.net, 2023a). Moreover, in 2022, the intentional access to websites containing child pornographic materials was defined as a criminal component, to be sanctioned with a fee not below 1000 EUROS and punished with reclusion for up to 2 years (Agenda Digitale, 2022).

To **report** an illegal website in Italy, the complaint must ultimately be made in person to the cyber police or other law enforcement. However, you can start the process online by submitting your personal information and details of the offence on the State Police website. After submission, you receive an electronic receipt and a protocol number to follow up in person. This online step does not replace the official complaint but serves as a preparatory draft. The report gains legal validity only once it is signed physically in front of a police officer. Therefore, the online form helps prepare and organise the complaint carefully, but the final formal complaint requires an in-person visit to law enforcement.

GREECE

In Greece, there are several ways to report content and/or request assistance, as outlined below:

- **Illegal or harmful content (e.g., child abuse, grooming, hate speech):**
  - Make a report via SafeLine.gr
  - Contact the Cyber Crime Division through the phone line 11188 or email
- **Revenge porn or non-consensual explicit content:**
  - File a complaint with the police
- **Minors' protection & parental controls to guide in cases of grooming or the solicitation of personal photos from minors:**
  - Use parco.gov.gr for guides and tools
- **Content removal (e.g., outdated or harmful search results) is valid in all countries:**
  - Submit a request through Google's Legal Help Center or Right to be Forgotten form

The following table presents the topic areas, pertaining legal frameworks, and the responsible Greek Authority.

Area	Legal/Policy Framework	Responsible Authority
Online platforms & intermediary services	Law 5099/2024, implementing the EU Digital Services Act (DSA), regulates illegal content, transparency, and user protection	Hellenic Telecommunications & Post Commission (HTPC) - Greece's authority overseeing compliance with the Digital Services Act, National Council for Radio and Television (NCRT), Hellenic Data Protection Authority (HDPA)
Pornographic websites & revenge porn	Article 346 of the Penal Code (Law 4947/2022) criminalises the non-	Hellenic Police Cyber Crime Division, Prosecutor's Office

	consensual distribution of intimate content	
Protection of minors online	National Strategy for Protection of Minors from Internet Addiction; includes parental controls, Kids Wallet app, and age verification	Ministry of Digital Governance, Ministry of Education, Hellenic Police Cyber Crime Division
Reporting illegal content (e.g., CSAM, hate speech, grooming)	SafeLine.gr (Greek Safer Internet Centre); INHOPE member; handles reports of illegal content	SafeLine Hotline, Hellenic Police Cyber Crime Division
Requesting content removal (right to be forgotten, harmful content)	GDPR & national privacy laws; Google's legal removal forms; SafeLine for illegal content	Google Legal Help Centre, SafeLine.gr, Hellenic Data Protection Authority

ESTONIA

In **Estonia**, the legal framework addressing online platforms, pornographic websites, and the protection of users—especially minors—is embedded within broader laws and policies focused on child protection, consumer rights, and digital safety, rather than in a single dedicated law.

Area	Legal/Policy Framework	Responsible Authority
Protection from violent/cruel content for children	Child Protection Act, Paragraph 25	Ministry of Social Affairs, Child Protection Agencies

Advertising restrictions targeting minors	Advertising Act	Consumer Protection and Technical Regulatory Authority
Restriction of hateful/violent content	Consumer Protection and Technical Regulatory Authority powers	Consumer Protection and Technical Regulatory Authority
Prevention of child sexual abuse online	Internal Security Development Plan 2025-2028	Ministry of the Interior
Implementation of the EU Digital Services Act	Ongoing national implementation	Consumer Protection and Technical Regulatory Authority
Data security and user protection	Electronic ID system, blockchain technology	Ministry of Justice and Digital Affairs, RIA (Information System Authority)

While there is no specific Estonian law solely regulating pornographic websites, the DSA and national laws require platforms to prevent access by minors to harmful content. The Media Services Act regulates audiovisual media services, including on-demand content, requiring registration and compliance with content standards. Age verification and restrictions on content harmful to minors are implied through these frameworks.

How to report, ask to remove the content, where and how to ask for help?

- Estonian Digital Services Coordinator: Under the EU Digital Services Act, Estonia's Consumer Protection and Technical Regulatory Authority acts as the coordinator for complaints about illegal content on large online platforms. Complaints can be submitted if platforms fail to remove harmful or illegal content, including online GBV.
- Police Reporting: Victims of online GBV can report crimes such as cyberstalking, threats, or distribution of non-consensual images to the Estonian Police. Law enforcement can investigate and take legal action.

Where to ask for help:

- Victim Support Crisis Helpline (116006): Available 24/7 in Estonian, English, and Russian, this free helpline provides confidential advice, emotional support, and guidance for victims of violence, including online GBV and sexual violence. It also offers information on legal rights and available services.

- Sexual Violence Crisis Centres: Specialised centres provide free, holistic care for victims of sexual violence, including those affected by online sexual harassment or abuse.

- "Notice. Intervene. Help." Campaign and Website: The Social Insurance Board is running a campaign focused on preventing sexual harassment, including online forms. The website www.palunabi.ee/ooelu offers practical tips for victims and bystanders on distinguishing harassment and how to intervene safely.

GUYANA

Guyana has made notable strides in building an interconnected response model that reflects a multidimensional approach.

Policy Frameworks

Guyana's legislative and policy landscape has evolved to provide stronger protections and accountability mechanisms:

- **Family Violence Act (2024)**: A landmark reform that integrates both criminal and civil remedies, empowering courts and police to intervene in domestic violence cases.

- **Sexual Offences Act (2010, amended 2013**) and Domestic Violence Act (1996, updated 2015): These laws form the backbone of legal protection for survivors.

- **National Gender Equality and Social Inclusion Policy (2018)**: Promotes legal reform, victim assistance, and public education to eliminate violence and discrimination.

Further, Guyana's GBV response is rooted in multi-sectoral coordination:

- **The Ministry of Human Services and Social Security** leads implementation through the Sexual Offences and Domestic Violence Policy Unit.

- **Guyana Police Force** now has expanded authority to intervene in private GBV cases, including arrest and removal of perpetrators.

- **Health sector** involvement includes medical symposiums and trauma-informed care training for professionals.
- **Community Advocate Network (CAN)** mobilises grassroots leaders to support survivors and raise awareness.
- **The 914 Hotline** offers rapid, confidential support to victims nationwide.

Guyana’s global partnerships pertain to the following:

- **Spotlight Initiative (EU & UN):** Guyana’s model, emerging from this initiative, is recognised as a regional leader in GBV response. It channels funding, technical support, and monitoring tools to local programs.
- **PANCAP and CARICOM frameworks**: Promote regional dialogue, data sharing, and policy harmonisation across Caribbean states.
- **Montevideo Strategy & Beijing +25 synergy:** Aligns Guyana’s efforts with global gender equality goals, including protections for Indigenous women and trafficking survivors.

DIGITAL EXPLOITATION IN PROSTITUTION AND CROSS-BORDER HUMAN TRAFFICKING

4. Digital exploitation in prostitution and cross-border human trafficking

Women's vulnerability to digital sexual exploitation is also rooted in structural inequalities. Limited access to education, high unemployment rates, poverty, and the subsequent scarce economic opportunities often constrain women's choices, pushing some toward online sexual content production (such as pornography, camming, or escort platforms) as one of the few available income sources. These risks are heightened for women who migrate for work or are displaced by conflict or environmental crises, as they often face legal precarity, language barriers, and the absence of support networks. A lack of resources and digital or sexual education further increases their exposure to deceptive recruitment and coercion. Understanding these systemic drivers is essential to addressing how digital platforms become sites of exploitation rather than empowerment.

4.1. Challenges of international cooperation

While international and cross-border cooperation in tackling online gender-based violence and digital exploitation of women is of the utmost importance, it is riddled with perplexities and gaps that pertain to differing legal frameworks, jurisdictional limits and obstacles, extradition policies, interoperability of databases, slow response times due to internal processes, and red tape, to mention a few.

- **Legal and jurisdictional barriers**: Since even legal definitions differ, countries may interpret concepts such as cyberviolence, consent, and digital exploitation differently. An act considered criminal in one jurisdiction may not (yet) exist in another country's legal framework, so that the act in question remains unregulated and unrestricted.

- **Cross-border legal ambiguity**: Since perpetrators often operate internationally, it can take time to determine which country has the authority to prosecute a specific criminal act. Defence attorneys use that to their advantage, inventing loopholes for the sole purpose of delaying justice.

- **Extradition limitations**: To date, many international treaties do not yet address cybercrime. Hence, even if extradition processes are in place, new treaties or additional protocols are needed so that victims can obtain legal recourse.

- **Law enforcement operational and administrative gaps and disparities**: Not all countries have the same infrastructure, training, capabilities, or expertise to tackle tech-enabled gender violence.

- **Challenges in collecting digital evidence**: Gathering digital evidence ready for prosecution across jurisdictions is both technically and legally complex.

- **Fragmented policies and coordination**: The lack of unified protocols and global standards for addressing online gender violence makes international efforts inconsistent and often ineffective. Central to this are data gaps; without harmonised data collection practices, said collection takes time, effort, and resources.

- **Underutilised civil society**: NGOs and grassroots organisations are often at the forefront of victim support and advocacy, and yet they are rarely integrated into formal international coordination mechanisms or consultation sessions.

- **Problematic platform accountability, transparency, and compliance**: There are services, websites, and applications that may operate beyond the reach of national laws, and may resist requests to remove harmful content or share user/possible criminal data. Here, of course, the dilemma of privacy versus accountability reappears; encryption and anonymity are definitely essential for women's safety online—but they also enable perpetrators and complicate investigations.

- **Absence of political will**: Some countries do not treat online gender violence and exploitation as the serious issue that it is; thus, they are not too prone to participate actively in cross-border initiatives.

4.2. The interplay with migration

Armed conflicts, climate change (loss of productivity, disasters, higher food prices), poverty and societal inequality are all among the root causes for migrating as well as exposing persons to the risk of trafficking and exploitation. Migrants are considered especially vulnerable to sexual exploitation and trafficking because of a combination of **structural, social, and personal risk factors** that traffickers actively exploit. These include legal and economic precarity, such as irregular or insecure legal status, financial vulnerability and in some cases, debt bondage. They also often lack knowledge of the host country's **language, rights, and legal protections,** which can prevent migrants from seeking help. Lack of access to accurate information makes it easier for traffickers to mislead them about job conditions or legal requirements. Migrants also often lack strong **social and family networks** in the host country, leaving them vulnerable to exploitation by recruiters, employers, or "community intermediaries." Migrants searching for jobs online or through informal social media groups are often targeted with **fake offers** (e.g., domestic work, hospitality, modelling) that turn into trafficking situations.

Globally speaking, the number of trafficking victims is on the rise since the COVID-19 pandemic, and child victims are increasingly detected. Girl and boy victims show different patterns of exploitation, with the majority of girl victims detected (60%) being trafficked for purposes of sexual exploitation, whereas this number is only 8% for boys. The same applies to women, for whom sexual exploitation accounts for 66%. This form of trafficking includes a variety of types of exploitation, from the forced prostitution of adults and the sexual exploitation of children to sexual slavery. Concerning digital exploitation, court case examples include cases of children exploited to produce child sexual abuse material, webcam shows and cybersex calls. (UNODC, *Global Report on Trafficking in Persons* (global datasets and analysis).

Digital platforms have become central to the facilitation of prostitution and trafficking. In some regions, social media accounts are associated with over **60**% of identified trafficking cases, and **77**% of traffickers target children using social media and other online tools. (https://endexploits.com/statistics.html)

Traffickers use classified ads and escort websites, social media and dating apps, messaging services and even darknet markets to recruit, advertise, control and exploit victims. International analyses have repeatedly found internet-enabled recruitment and advertising in trafficking cases; for example, UNODC case-data studies and OSCE mapping identify escort sites, massage/sexual-services websites and social media as common channels. In the United States, the National Human Trafficking Hotline and Polaris have documented hundreds of instances of online recruitment and identified thousands of contacts linked to technology-enabled trafficking. Polaris reports that since 2015, the hotline has flagged **more than 950 potential sex-trafficking victims** who were recruited online. Digital tools shift how coercion and control are applied (remote grooming, deceptive ads, monitoring via messaging apps, and payment funnels), and also complicate responses because platforms cross borders and operate under varied legal regimes.

Digital platforms used for sexual exploitation

Digital tools and online platforms are extensively used in sexual exploitation worldwide, as many platforms lack moderation, reporting mechanisms and transparency in how they respond to exploitation cases. For example, OnlyFans submitted **230 reports** to the National Center for Missing & Exploited Children (NCMEC), with **64 additional reports** filed by February 2025—highlighting ongoing challenges in detecting underage content.

https://www.statista.com/statistics/1339631/onlyfans-reports-to-national-center-missing-exploited-children-csam-material/?utm_source=chatgpt.com)

They also receive recurring complaints about explicit content involving individuals who have been posted on the platform without their consent.

https://nypost.com/2024/03/13/us-news/behind-the-onlyfans-porn-boom-inside-allegations-of-rape-abuse-and-betrayal/

In August 2025, the UK's anti-slavery commissioner launched an inquiry into escort/ad sites (e.g., Vivastreet), described as "pimping websites." A 2021 Scottish study noted how such platforms have "turbocharged the sex-trafficking trade."

https://www.theguardian.com/society/2025/aug/30/uk-anti-slavery-commissioner-launches-investigation-into-pimping-websites

In addition to escorting and adult content platforms, traffickers also massively use mainstream social media platforms such as Tinder, Instagram and TikTok, as well as online marketplaces and even online game platforms such as Roblox, Minecraft or Hago. Platforms that combine popularity among young people with social features (such as chat, voice, avatars, and in-game rewards) have become fertile ground for abuse. The scale of grooming, the speed at which it unfolds, and its frequent linkage to platforms outside the games themselves (like Discord or Snapchat) underscore a pressing need for improved safety design, moderation systems, and parental/educator awareness. Gaming platforms are especially used to target youngsters and children. Exploitation reports on Roblox have surged from **675 in 2019 to over 24,000 by 2024**, spotlighting the scale of the problem.

https://www.wired.com/story/is-roblox-getting-worse/?)

- **Social Media & Messaging Apps**

Traffickers use mainstream platforms like Facebook, Instagram, TikTok, LinkedIn, WhatsApp, and Telegram to recruit, groom, and control victims. They often pose as friends, romantic interests, or job recruiters. They allow for easy targeting of vulnerable individuals and private communication channels that conceal exploitation. Instagram profiles can be disguised as escort ads, with contact details in bios or stories. NGOs in France and the UK have documented traffickers creating fake "modelling agencies" on Instagram to lure young women. On LinkedIn or Indeed, traffickers pose as recruiters or HR managers, contacting young or unemployed people directly, offering, e.g "work abroad" or "high earnings with no experience needed".

- **Online gaming platforms**

Online game platforms have been misused for grooming, coercing, or otherwise exploiting children and teenagers sexually. Predators meet victims through games and can coerce them to share explicit material or meet in person. Adults have been reported to lure children using the in-game currencies (such as Robux of Roblox) and then directing them to apps like Discord or Snapchat for exploitation.

- **Dating & Escort Websites**

Websites and apps designed for dating (e.g., Tinder, Bumble) or commercial sex/escort services are often used to advertise victims under coercion. Ads may disguise exploitation as consensual sex work, making detection difficult. Traffickers on Tinder may pose as potential partners, building trust before manipulating victims into sexual exploitation. They exploit Tinder's location-based matching to identify vulnerable people (migrants, refugees, travellers) in border areas or new host countries, offering "help" or "jobs" that lead to exploitation, such as providing modelling or sugar-baby opportunities.

- **Classifieds & Online Marketplaces**

Some traffickers post misleading job ads (e.g., modelling, hospitality, au pair work) on global classifieds ads marketplaces or local equivalents. Victims may be lured into exploitative situations under the guise of legitimate employment. Fake ads for rooms, second-hand goods, or "friendship" can serve as entry points for traffickers to identify and approach vulnerable individuals. Migrants seeking affordable housing on Facebook Marketplace, for example, have been targeted with "offers" tied to sexual exploitation.

- **Live-Streaming & Adult Content Platforms**

Traffickers exploit victims through live-streamed sexual acts on camming sites or upload coerced content to subscription platforms. Traffickers force victims (including children, migrants, or vulnerable adults) to perform on camera under threat, violence, or debt bondage. Victims may be locked in rooms, monitored, or denied earnings, while traffickers control the accounts. In some cases, traffickers force victims to meet clients offline after online "shows" as a pipeline to in-person prostitution. The platforms can also be used for "sextortion". Audiences or traffickers record victims without consent and use footage for blackmail ("perform again or this goes public").

- **Darknet Markets & Encrypted Services**

Hidden services on the darknet facilitate advertising and distribution of exploitative material. Law enforcement faces challenges in monitoring these hidden markets.

Protective measures

Protecting individuals requires a multi-pronged strategy: robust platform moderation and mandatory reporting, tech-enhanced detection for law enforcement, regulation of adult-service platforms, and empowerment resources for creators, youth, and vulnerable populations.

Platforms should be legally obligated to flag suspicious activity to authorities, demand proactive ID checks, implement robust image/video screening, and submit to audits on how they handle exploitation complaints. Escort websites should be regulated to prevent misuse, and law enforcement should use Artificial Intelligence-driven detection tools to identify trafficking patterns in escort ads.

Migrants can be better protected by increasing awareness and information on the risks of online recruitment scams and sexual exploitation. Community centres, NGOs, and local services should teach migrants how to verify online offers, protect their privacy, and use platforms safely. Workshops or peer-to-peer education, engaging migrant community leaders, are among the good practices. The contents should be clear and culturally adapted.

Especially youth and children need to be aware of online grooming tactics and "red flags" (e.g., pressure to keep conversations secret, requests for intimate images), and parents need to be made aware of the importance of parental controls, privacy filters, and platform safety features. Awareness campaigns on these subjects in schools, other educational environments and the media are needed, as well as educating social and education workers.

A Case Study: Migration in Guyana

Migration in Guyana is a complex and historically significant occurrence that has shaped the country's demographics, economy, and global connections.

The intersection of migration, environmental pressures, and digital exploitation in Guyana reveals a layered set of challenges—especially for vulnerable populations in hinterland and coastal regions.

Digital exploitation risks

As migration increases—especially among youth and women—digital platforms become both lifelines and potential traps:

- Online Recruitment Scams: Migrants seeking jobs abroad or in urban areas may fall prey to fraudulent online offers, leading to trafficking or labour exploitation.
- Data Vulnerability: Limited digital literacy makes migrants susceptible to identity theft, phishing, and misuse of personal information.
- Gendered Exploitation: Women and girls migrating for work or education face heightened risks of sextortion, cyberbullying, and online harassment.

Difficulties and challenges in Guyana

- Digital Divide: Hinterland and Indigenous communities often lack reliable internet access, making them digitally invisible and vulnerable.
- Limited Legal Protections**:** Guyana's migration and digital safety frameworks are still evolving, leaving gaps in protection for individuals displaced by climate change and those vulnerable to digital exploitation.

- Trust & Cultural Barriers: Studies show that trust in e-government services is low, and cultural factors hinder the adoption of digital safeguards.
- Geopolitical Pressures: Territorial disputes and labour market shifts add complexity to migration governance.

Emerging solutions

- ICT Hubs in Hinterland Regions: Over 200 hubs have been established to improve digital access, education, and early warning systems for climate events.
- E-Government Expansion: Guyana is investing in digital governance to improve service delivery and reduce exploitation risks.
- Diaspora Engagement: Programs are being developed to harness the skills and resources of Guyanese abroad, while protecting those who migrate.

The rapid expansion of digital infrastructure in Guyana has brought both opportunities and risks. While digital tools have empowered citizens and improved public services, they have also been weaponised for exploitation.

Digital tools are most used for exploitation in Guyana

Social Media Platforms (Facebook, WhatsApp, Instagram): Used for phishing, impersonation, sextortion, and recruitment scams. Exploiters often pose as employers, romantic interests, or government agents to gain trust and access personal data.

- Phishing Emails & Malicious Links: Sent via email or messaging apps, these links trick users into revealing passwords or downloading malware. Common scams include fake bank alerts, job offers, or government notices.
- Botnets and Malware: Criminals use infected devices to launch remote attacks or steal data. These networks can be used for identity theft, financial fraud, or to spread illegal content.
- Social Engineering Tools: Exploiters use publicly available data to manipulate victims through phone calls or direct messages. They often impersonate customer service agents or officials to extract sensitive information.
- Spyware & PUPs (Potentially Unwanted Programs): These are hidden in downloads and can monitor user activity, steal data, or disable security features.

Protective measures

- Cybersecurity Policies & Legislation**:** Guyana has implemented 43 cybersecurity policies across government agencies to safeguard digital infrastructure. Laws like the Data Protection Act and Digital Identity Card Act aim to protect user privacy and secure online transactions.

- National Cybersecurity Training: Public servants are being trained to detect and respond to cyber threats. Events like the Cybersecurity Fair bring together experts for workshops and live demonstrations.
- Smart Public Systems: Systems like Safe Road Intelligent e-ticketing, automated border control, and electronic health records are designed with built-in security protocols.

- ICT Master Plan (2030). This strategic roadmap focuses on digital efficiency, security, and resilience across sectors. It includes monitoring systems, evaluation frameworks, and progressive technologies to detect and prevent cybercrime.

- Community Awareness & Education: NGOs and government agencies are working to improve digital literacy, particularly in rural and vulnerable communities. Awareness campaigns target youth and women, who are disproportionately affected by digital exploitation.

4.3. Educating communities on digital safety

While online platforms are increasingly becoming a central part of our lives, they can also pose serious risks if not used responsibly. New information and communication technologies have revolutionised media distribution, access to information, and global communication. However, these same technologies can facilitate sexual exploitation on local, national, and international levels (Hughes, 2002).

It is therefore essential that all community stakeholders prioritise digital safety. This includes educating themselves using up-to-date resources to combat online violence and equipping minors and youth with knowledge about digital risks and prevention strategies. In educational settings, teachers play a pivotal role in strengthening digital literacy; a competent and intentional educator is key (Tomczyk, 2019). Policymakers must also recognise children as active participants in the digital world who can engage meaningfully with information (Patterson et al., 2022).

Overall, the aim of digital literacy in the context of internet safety is to promote safe, creative, and informed use of digital media (Kurniasih, 2023). While many internet safety initiatives have emerged over the past two decades to encourage responsible online behaviour, there is still room for improvement in their delivery methods (Quayle, 2020). Depending on the target audience, resources range from interactive to explanatory, each offering valuable opportunities for engagement.

Digital platforms have become central to young people's daily lives. They offer opportunities for learning and communication, but, as mentioned above, also expose minors to significant risks, including **cyberbullying, exposure to harmful content, and sexual exploitation** (Hughes, 2002).

Protecting children online requires **community-wide engagement**. Schools, families, and local authorities all have a role in **building digital literacy and awareness**:

- **Teachers** can equip students to recognise online risks and respond effectively (Tomczyk, 2019).
- **Parents and caregivers** need practical guidance to mediate screen use and discuss online experiences openly.
- **Policymakers** must ensure children are recognised as **active digital citizens** and supported by **robust protective measures** (Patterson et al., 2022).

Recent studies illustrate the **scale and urgency** of this challenge.

Key Figures: Online Risks for Young People

Risk Area	Key Statistics	Sources
Cyberbullying	15% of adolescents (≈1 in 6) have experienced cyberbullying; 29% in high school	Santé Mentale, (2024); Jedha, (2025)
Harmful Content Exposure	Average first exposure to pornography: **10 years old**; 70% of 11–18-year-olds have seen disturbing content (violence, pornography, war images)	Élysée Report, (2023); Le Monde, (2024)
Screen Time	Ages 6–17: **4h11/day**; Teens 13–19: **7h+/day**; 57% of under-20s report negative effects	GoStudent, (2025); INSEE, (2024)

These trends highlight the **growing digital vulnerability of youth**. Effective digital education is not only a protective measure; it **supports healthy, informed, and creative participation** in the online world (Kurniasih, 2023).

To be effective, community strategies should include:

- **Early intervention in schools**, starting in primary education.

- **Parental engagement and awareness campaigns** to reduce early exposure to harmful content.
- **Clear policy frameworks** linking child protection, media literacy, and public health.

By combining **education, prevention, and policy action**, communities can create **safer and more empowering digital environments** for children and adolescents.

Educational digital safety campaigns

EU-wide video campaigns

- 58Deutsche Telekom's campaign "Share with Care" for sharing pictures and videos of children online: https://youtu.be/F4WZ_k0vUDM
- Europol's "Say No" campaign for catfishing and sexual extortion:
- https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime.

Examples of resources on the digital safety of migrants

- **MIDEQ – Training on Safe, Wise, and Secure Use of Digital Technology**

Language: English. A freely accessible slide deck and facilitator notes, licensed under a Creative Commons license, designed to empower women and girls migrants in Southern Africa. Topics include online harassment, scams, identity theft, and misinformation.

https://www.mideq.org/en/impact/impact-resources/training-on-safe-wise-and-secure-use-of-digital-technology/

- **Tabliteracy – Digital Citizens Course (Ireland)**

Language: English (designed for learners with lower English proficiency). A tablet-based curriculum teaching device uses online safety, job searching, finding services, communication tools, and local integration in Ireland. It's activity-based and tailored to real-life needs.

GREECE

Digital Safety Campaigns in Greece for Youth

The Greek Safer Internet Centre has launched several impactful campaigns and provided pertinent resources:

- **Safer Internet Day Contests**: Over eight hundred (800) schools participated in creating digital content on cyberbullying, misinformation, and online fraud.
- **Capture the Flag (CTF) Contest**: Introduced students to cybersecurity through hands-on challenges in cryptography and digital forensics.
- **Back-to-School Packages**: These include resources such as lesson plans, quizzes, videos, posters, and fairy tales tailored for different age groups.

Digital Safety Campaigns for Adults:

National Strategy for Media Literacy & Digital Skills

Central objectives:

- To promote the safety of digital technologies
- To offer related learning opportunities for adults

European Safe Online Initiative

This is an interactive project designed for both parents and teachers to educate them on the risks associated with digital media. It provides resources on:

- Cyberbullying
- Internet privacy
- Social media issues

ESTONIA

In Estonia, several national initiatives promote digital safety and media literacy among children, young people, adult women, and migrant communities. These initiatives provide schools and community organisations with practical resources, lesson plans, workshops, and awareness campaigns.

- **Targalt Internetis (Smartly on the Web)**

Estonia's Safer Internet Centre, coordinated by Harno and the Estonian Union for Child Welfare. Provides:

  - Free lesson plans, interactive games, and videos on topics such as cyberbullying, grooming, privacy, and digital footprints.
  - Classroom workshops and school visits are delivered by trained experts.
  - Training sessions for teachers, youth workers, and parents.

- **Inspiratsioonikogumik**

A toolkit published by Targalt Internetis offering ready-made activities for teachers. It includes:

  - Classroom exercises on cyberbullying, online ethics, and digital footprints.
  - Adaptable templates for workshops with young people and migrant groups.
  - Practical guides for addressing harmful online content.

- **Lasteabi (Child Helpline 116111)**

Offers educational materials and confidential counselling to children and families Educators can:

  - Use their online modules on recognising and reporting online harms.
  - Invite counsellors to give talks in schools or youth centres.
  - Access multilingual guidance materials for migrant families.

- **Safer Internet Day campaigns (coordinated by Harno and supported by Telia Estonia)**

Each February, Estonian schools, kindergartens, libraries, and youth centres participate in nationwide awareness-raising activities coordinated through Targalt Internetis. In 2024, over 7,600 children took part in 70 events. Educators received thematic material packages (videos, online tests, games) to run classroom sessions and discussions. The leading conference, *"Smartly on the Web: Digital Well-being and Mental Health"*, included workshops presenting new tools like **ySKILLS**, **Triumfland Saga**, and **Spoofy**. The campaign also introduced a **cybersecurity quiz ("KüberNööpnõel (CyberPin)")** for grades 1–6 and a **digital escape-room competition** for grades 7–12.

France

French best practices and practical activities

Cybermalveillance.gouv.fr – "Cyber Guide Famille" and Youth Campaigns

- Offers educational tools like comics, quizzes, motion-design videos, and a "As du Web" vacation workbook tailored for 7–14-year-olds.
- Activities can be adapted in class: interactive quizzes, scenario-based discussions, and "digital super-hero" identity exercises. Assurance Prévention+7Education Ministère+7cnil.fr+7CYBERMALVEILLANCE.GOUV.FR

CNIL – Data Protection Workshops & Games

- Provides age-specific kits ("Tous ensemble, prudence sur Internet !") for CE2–CM2 and 11–15-year-olds.
- Includes games, videos, printable activities and "Incollables®" booklets to teach personal data protection through playful challenges.
- Educators can use these as classroom modules or assign parental workshops. cnil.fr+1CYBERMALVEILLANCE.GOUV.FR+1

Internet Sans Crainte / Safer Internet Day France

- Annual Safer Internet Day workshops with themed kits (e.g. *AI & digital citizenship*, *escape games like "Vinz et Lou"*).
- Ready-to-use modules for cycle 2, 3, and high school, designed for classroom delivery or peer-led sessions. CYBERMALVEILLANCE.GOUV.FR+3Better Internet for Kids+3Teachit+3

Promeneurs du Net (PdN) – Digital Mentorship

- Professional youth workers engage online to support 12– to 25-year-olds through a structured online presence.
- Activities include moderated chat sessions, peer discussion groups on digital risks, role-play simulations, and Q&A sessions in youth centres or online. Wikipedia

CLEMI – Media Literacy and Critical Thinking Workshops

- Through the Ministry-run network, CLEMI provides lesson plans and fact sheets for media literacy education, including social media analysis, detecting fake news, and civic use of media.
- Teachers run projects like student newspapers or photo/media decoding exercises to develop critical digital skills. Wikipedia

Académie de Créteil – "Forming à la cybersécurité" Guide

- A 13-sheet booklet for schools covering: basics of cybersecurity, protecting data, identifying phishing attempts, and secure device habits.
- Designed for group work or workshops in collège / lycée. Better Internet for Kids+2dane.ac-creteil.fr+2Assurance Prévention+2cnil.fr

CNIL's 8 Recommendations – Co-designed Child Workshops

- CNIL developed and co-created workshops with children to explain concepts such as consent, privacy rights, and safe autonomy.
- Suggested format: interactive sessions where teens contribute to designing UI flows or messaging they would understand. cnil.fr

Kit pédagogique du citoyen numérique (CNIL, Arcom, HADOPI, Défenseur des droits)

A freely available, downloadable set of educational materials (videos, infographics, slides) to teach digital citizenship—covering privacy, online rights, distinguishing legal and illegal content, and media literacy. Great for facilitators working with migrants. Portail pédagogique

- **ContreLaTraite.org – Resource Centre**

An extensive online resource repository (in French) with e-learning, guides, campaigns, and support for professionals—especially on trafficking in contexts affecting migrants. Offers a broad array of materials—training, prevention tools, campaign information—that can be adapted or used directly in migrant-focused programs. https://contrelatraite.org/centre-ressources

- **Ressources de médiation numérique (Les Bases du numérique d'intérêt général)**

A rich repository featuring tools and guides to accompany vulnerable people digitally—including cybersecurity, digital mediation, parental support, and multimedia learning games. https://lesbases.anct.gouv.fr/ressources/ressources-pedagogiques

- **Mouvement du Nid - "Y'a quoi dans ma banane?"**

Designed for young people aged 12 and over, this virtual belt bag contains accessories—a phone, keys, notebook, etc.—that serve as tools for learning about and reflecting on a range of topics related to emotional and sexual life, gender equality, and gender-based and sexual violence, including prostitution and sexual exploitation. https://dansmabanane.mouvementdunid.org/

Trousse pour les jeunes – Sécurité en ligne (Canada)

Aimed at adolescents (13–14 years), this Canadian toolkit explains forms of online sexual exploitation such as sexting, sextortion, capping, and grooming, with slides, presenter notes, and tips to encourage victims to speak out. Gouvernement du Canada

Malettes pédagogiques – CVM (Collectif contre la violence du marché sexuel)

These digital "toolkits" provide materials for parents and professionals to address and prevent child prostitution—featuring videos, guides, and awareness resources. association-cvm.org Droit d'Enfance

Sample Classroom Activities

Age range	Activity	Objective	Format
7–11 yrs	Comic-strip creation: depict safe vs unsafe messaging	Understand privacy & digital conduct	Group work & presentation
11–15 yrs	Escape game “Get me out of AI” (Vinz et Lou)	Recognise AI risks & digital citizenship	Roleplay game
Collège/Lycée	Fake news workshop with CLEMI sheets	Develop critical thinking and media literacy	Classroom debate & digital production
Teens online	Live session with Promeneurs du Net	Open dialogue on cyberbullying, privacy, and sexting	Moderated chat
Parent & child	CNIL data-protection family quiz	Stimulate discussion at home and school	Take-home booklet/workshop

How to Use These Resources Effectively

- Mix educational formats: Combine videos, interactive quizzes, comics, group discussion, physical activities, and digital tasks.

- Co-create content: Let youth design their own safety posters, media campaigns, or UX flows for privacy settings, with teacher facilitation.
- Involve parents: Offer take-home kits or joint workshops (e.g. CNIL booklets or Cyber Guide briefs).
- Use peer mentors: Involve young "digital ambassadors" from PdN or Safer Internet Day teams to lead sessions.
- Build progression: Start with simple concepts (e.g., privacy basics at primary school) and evolve to more complex topics, such as misinformation and AI, at a secondary level.

ITALY

- **BEAWARE** Project (France, Italy, Greece, Portugal, Belgium, Cyprus): *Understanding, preventing, detecting and addressing Online Sexual Exploitation and Abuse (OSEA) through a holistic, multi-faceted and multisectoral approach.* **Resources:**
    - The toolkit for educators is designed to provide theoretical insights into topics related to online safety, risks, and dangers on online platforms. It also gives practical suggestions on how to address episodes of online abuse and how to relate to the young person who is reporting.
    - The mobile app for youth addresses different topics through interactive challenges. This can also be used in groups.
    - The learning platform is an online space for youth workers and educators to gain a broader understanding of digital literacy on relevant topics and become more aware of how to address these issues when interacting with young people.
- **CESAGRAM** Project (Belgium, Greece, Italy, UK, Lithuania): *Enhancing the understanding of the process of grooming, and more particularly how it is facilitated by technology and how it can lead to child sexual abuse and missing.* **Resources**:
    - The library has a multitude of sources to retrieve and get informed.
    - Useful Consultation for Parents on Technology-assisted Child Sexual Abuse materials for parents on online safety.
    - Mapping of expert organisations' practical information on where to get support and more knowledge on the matter.

CAMPAIGNS:

National initiatives in Italy

In the course of their lives, according to the National Institute of Statistics, 6.8 per cent of women have had inappropriate propositions or obscene or malicious comments made about them through social networks (Consiglio Regionale del Piemonte, 2022). The prevalence of online harassment is increasing, consistent with the growing use of social networks in recent years. More than 44% of harassment on social media was repeated multiple times in the case of female victims (ibidem). Nonetheless, despite the growing alarm on the phenomenon, initiatives are still wide and not as specific as they should be in the digital dimension and its risks (Lavoce.info, 2025). In Italy, women can rely on effective and very renowned support systems to address episodes of online violence, too.

- **1522 hotline**

  National 24-hour toll-free phone number for support and information in cases of violence or stalking. The service is anonymous and confidential.

- **Telefono Rosa (The Pink Telephone) 06.37.51.82.82**

  It was made available by the National Association of Volunteers of Telefono Rosa Onlus (www.telefonorosa.it). Also operating 24 hours a day, the service aims to provide assistance, support and counselling to women victims of violence or any form of abuse by offering attentive and qualified listening and support in understanding their rights and possible actions to take to get out of the dangerous situation.

No targeted governmental campaigns were found in Italy. However, NGOs do indeed work on the prevention of online gender based violence; below is a recap of some of the most relevant.

- The CONVEY project aimed to combat sexual violence and harassment against women by promoting peer-to-peer education among young people. It focused on raising awareness about the impact of gender stereotypes and sexualisation in digital media. Through the development of an educational simulation game and a pilot programme on gender equality, sexual education, and media literacy, the project encouraged behavioural change. CONVEY also supported teachers with a train-the-trainer programme, helping schools foster respect for women's rights and prevent gender stereotyping in today's digital society while developing policy recommendations.

- The CHASE project aimed to address the growing issue of online gender-based hate speech by developing and implementing a comprehensive response mechanism in Cyprus, Italy, Greece, and France. It focused on improving detection and reaction strategies within online media platforms. Recognising the lack of gender-disaggregated data and limited research on cyber violence, CHASE sought to fill these gaps and support the creation of safer digital spaces. The project contributes to more effective, coordinated EU policies against online gender-based violence and hate speech.
- EmpowerTech is a digital training project promoted by D.i.Re and the University of Calabria, designed for activists working in Anti-Violence Centres. The program is conducted online and focuses on three main goals: improving security in managing sensitive data and using digital tools consciously; increasing work efficiency through the use of free and open-source digital tools; and promoting personal and collective well-being through techniques to reduce stress and enhance collaboration. The initiative aims to strengthen the digital skills of activists, fostering a safer, more effective, and more supportive working environment.

- **"LET'S TALK ABOUT IT"** – *Parliamone!*
  A project launched in a Palermo high school, including a **digital manual** for youth workers to address LGBTQIA+ bullying and cyberbullying.

- **Differenza Donna school projects -** A range of initiatives (2008–2023) preventing aggressive behaviour and promoting gender equality education in primary and secondary schools in Rome, including *Schools in Network Against Violence*, *Pari e Dispari*, and *Facciamo la differenza*.

- **ADA Project – Increasing Digital Skills in Anti-Violence Centres,** Funded by the *Fondo per la Repubblica Digitale* (2025–2026), this project equips staff at anti-violence centres with digital skills, focusing on online gender-based violence, activism, and digital communication.

- **Safer Internet Day / Generazioni Connesse,** an international awareness day (second week of February) dedicated to online safety, coordinated in Italy by **Generazioni Connesse** in collaboration with the Ministry of Education, Postal Police, Save the Children, and other partners.

- **Una vita da social** (*A Social Life*), A travelling campaign by the **Italian State Police**, part of the Generazioni Connesse project, aims to raise awareness among students, teachers, and families about the risks of the internet, meeting millions of people in schools and public squares.

- **Noi cittadini digitali** (*We Digital Citizens*), an initiative by **Trend Micro** and **JA Italia** aimed at developing a conscious culture of Internet use. It offers workshops for middle school students and issues a "digital citizenship license" on Safer Internet Day.
- **Cybercity Chronicles – "Be Aware Digital" campaign,** an educational video game ("edutainment") created by the **DIS** (Italian Intelligence Department) with the Ministry of Education to raise awareness among lower secondary school students about online risks.

4.4. The Private Sector's Impact

Far from being passive platforms, today's tech companies are active stewards of digital safety. Social media networks, messaging apps, and other online services have evolved into frontline defenders against gender-based cyber harms. Their role as gatekeepers is not just regulatory—it is at times visionary. By refining algorithms, enhancing moderation protocols, and safeguarding user data, these firms not only mitigate abuse but also often anticipate it before it escalates. The private sector's agility enables it to respond more quickly than legislation ever could, adapting to emerging threats with precision and scale.

Designing with Empathy and Foresight

Ethical design is not just a mere requirement, but also a competitive advantage. Forward-thinking companies are embedding gender-sensitive principles directly into their product development cycles. This means building features that discourage stalking, harassment, and non-consensual data sharing, while promoting user autonomy and safety. Unlike bureaucratic mandates, these innovations are driven by market responsiveness and a genuine desire to serve diverse user bases. The private sector's ability to iterate quickly ensures that ethical considerations are functional, user-tested, and – thus - impactful.

Accountability as a Business Imperative

Transparency is a fundamental imperative of business ethics. Tech firms increasingly publish detailed reports on abuse cases, moderation outcomes, and user safety metrics, not because they are forced to, but because trust is their currency. Ethical audits and third-party reviews are becoming standard practice, reinforcing the sector's commitment to fundamental rights. In many cases, companies are setting the bar higher than regulators require, proving that accountability can be a self-driven pursuit rather than a reactive obligation.

Strategic Collaboration with Civil Society Actors and Grassroots organisations

Private companies are not working in isolation. They are forging powerful alliances with NGOs and advocacy groups. These partnerships have led to the development of smarter reporting tools, more empathetic support systems for survivors, and awareness campaigns that resonate globally. The corporate realm brings scale, infrastructure, and technical expertise; civil society brings lived experience and grassroots insight. Together, they are bridging capability gaps and further building entirely new frameworks for digital safety and security.

Moreover, training programs led by NGOs are helping developers and moderators internalise gender sensitivity; however, it is the companies themselves that are investing in these efforts, recognising that inclusive platforms are more sustainable and more profitable. Even in policy advocacy, the private sector is no longer a reluctant participant but a proactive ally, lending its voice and resources to shape legislation that reflects the real-world dynamics of digital technology.

Innovation as a Shield Against Exploitation

The private sector's most powerful contribution to digital safety lies in its capacity for innovation. AI-powered moderation tools now detect abusive language, image-based exploitation, and coordinated harassment in real time, a feat that humans could not achieve at scale. These technologies are also predictive, learning from patterns to prevent harm before it happens (and not just reacting to perpetrating acts).

Privacy-first design is another hallmark of corporate ingenuity. End-to-end encrypted direct messaging, anonymous reporting, and customisable visibility settings empower users to reclaim control over their digital lives. These are not fringe but core features, shaped by user demand and ethical foresight. Furthermore, when it comes to data protection, companies are leaders through robust encryption, minimal third-party access, and internal safeguards – all of which are becoming industry norms, especially when it comes to sensitive data such as reproductive health or location tracking.

CONCLUSIONS

5. Conclusions

In the constant struggle to protect women from online exploitation, associations and advocacy groups are confronting a system that is often structurally unprepared for the realities and evolution of digital crime. Traffickers operate with a degree of impunity across borders, exploiting the absence of cohesive international law and the inertia of judicial cooperation among countries. While the internet knows no boundaries, penal justice systems remain at their core national and thus slow to communicate, reluctant to collaborate, and at times paralysed by incompatible legal definitions of trafficking, consent, and digital abuse.

For women who are targeted, the consequences are devastating. Survivors are left waiting for long periods of time for courts to determine jurisdiction, for evidence to be admissible, and for foreign authorities to respond. Associations working on their behalf must navigate a complex web of bureaucratic red tape, often relying on informal networks and personal relationships to advance cases. The lack of urgency in cross-border cooperation halts processes.

Adding to this complexity is the opaque world of cryptocurrency. Traffickers are increasingly using Bitcoin and other digital currencies to move money anonymously, thereby bypassing traditional financial systems and evading detection. While blockchain offers theoretical traceability, in practice, the tools required to follow these trails are expensive, highly technical, and often out of reach for Law Enforcement. Privacy coins, mixers, and decentralised exchanges further obscure financial transactions, allowing perpetrators to launder profits with minimal risk.

Women's safety online cannot be an afterthought. It must be a central pillar of digital governance. That means building international legal frameworks that prioritise vulnerable populations and human rights. This means investing in cross-border judicial training, shared databases, and rapid-response protocols. It also involves regulating 'crypto' markets with the same vigilance applied to traditional finance—because when money moves in the shadows, so does female exploitation.

One should remember that online sexual exploitation does not occur in a vacuum; it is deeply embedded in and sustained by structures that profit from attention, engagement, and control. Social media platforms and digital services are designed to prioritise profit over safety, often amplifying sensational, violent, or sexualised content to maximise user engagement. Exploitative industries — from pornography to data harvesting — capitalise on the commodification of women's bodies, private lives, and emotional vulnerability. In this system, gendered abuse is not a glitch but a feature: a profitable byproduct of a digital economy that values virality over accountability and exposure over consent.

Until all these systems evolve, associations will continue to fight uphill battles with limited tools and boundless determination. Their work is not just about justice—it is about restoring dignity to women who were preyed on the internet – a space otherwise designed for freedom and connection.

BIBLIOGRAPHY

6. Bibliography

60 Statistiques sur le temps d'écran des enfants en 2025. (n.d.). GoStudent. https://www.gostudent.org/fr-fr/blog/statistiques-temps-ecran-enfants
Acquaviva, M. (2022, April 15).
Come segnalare un sito dai contenuti illegali? La Legge per Tutti.
https://www.laleggepertutti.it/539189_come-segnalare-un-sito-dai-contenuti-illegali*Anonymity and identity shielding*. (2025, May 28).
eSafetyCommissioner. https://www.esafety.gov.au/industry/tech-trends-and-challenges/anonymityCamarda , C. (2023, October 27).
La pedopornografia e i reati informatici minorili. Diritto.net.
https://www.diritto.net/pedopornografia/
Carcelén-García, S., Narros-González, M. J., & Galmes-Cerezo, M. (2023). Digital vulnerability in young people: gender, age and online participation patterns. *International Journal of Adolescence and Youth*, *28*(1).
https://doi.org/10.1080/02673843.2023.2287115
Cyber Security Challenge Greece. (n.d.).
https://cybersecuritychallenge.gr/2025/
Cyberviolence against women in the EU. (2024). In *European Parliament*.
https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI(2024)767146_EN.pdf
Digiturvalisuse mängud. (n.d.). *Digiturvalisuse mängud*. Digiturvalisuse Mängud. https://www.lasteaeg.ee/
En 2023, un tiers des internautes ressentent au moins un effet néfaste des écrans - Insee Focus - 329. (n.d.).
https://www.insee.fr/fr/statistiques/8199393
FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women | UN Women – Headquarters. (2025, February 10). UN Women – Headquarters.
https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women

Fournari, J. (2025, April 9). *Chiffres sur le cyberharcèlement en 2025*. Jedha. https://www.jedha.co/formation-cybersecurite/chiffres-sur-le-cyberharcelement-en-2025

Goal 5 | Department of Economic and Social Affairs. (n.d.). https://sdgs.un.org/goals/goal5

Greek Safer Internet Centre. (n.d.). Better Internet for Kids. https://better-internet-for-kids.europa.eu/en/sic/greece

Guyana Gender-based Violence Policy Brief – PANCAP. (n.d.). https://pancap.org/pancap-documents/guyana-gender-based-violence-policy-brief/

Guyana has comprehensive, holistic model to address Gender-Based Violence. (2024, September 22). DPI Guyana. https://dpi.gov.gy/guyana-has-comprehensive-holistic-model-to-address-gender-based-violence/

How Technology-Facilitated Gender-Based Violence Impacts Women and Girls. (2023, November). United Nations - Regional Information Centre for Western Europe. https://unric.org/en/how-technology-facilitated-gender-based-violence-impacts-women-and-girls/

Inicio. (n.d.). Comisión Económica Para América Latina Y El Caribe. http://www.cepal.org/

Inspiratsioonikogumik 2023 - targalt internetis. (2024, January 16). Targalt Internetis. https://www.targaltinternetis.ee/inspiratsioonikogumik-2023/

Komal. (2025, March 27). *The impact of social media in combating Gender-Based Violence*. IJLSSS. https://ijlsss.com/the-impact-of-social-media-in-combating-gender-based-violence/

L'Hoiry, X., Moretti, A., & Antonopoulos, G. A. (2024). Human trafficking, sexual exploitation and digital technologies. *Trends in Organized Crime*, *27*(1), 1–9. https://doi.org/10.1007/s12117-024-09526-4

Marasco, T. (2019, March 11). *È legale vedere video pornografici su internet?* La Legge per Tutti. https://www.laleggepertutti.it/104726_e-legale-vedere-video-pornografici-su-internet

Ministry of Digital Governance. (n.d.). *THE GREEK NATIONAL DIGITAL DECADE STRATEGIC ROADMAP*.

https://digitalstrategy.gov.gr/website/static/website/assets/uploads/digital_decade_national_roadmap.pdf

Open Access Journals | Texila International Journal. (n.d.). http://www.texilajournal.com/

Ourania. (2022, October 11). *European SafeOnline Initiative – (ESOI)*. Athens Lifelong Learning Institute. https://athenslifelonglearning.gr/el/european-safeonline-initiative/

Quayle, E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. *ERA Forum*, *21*(3), 429–447. https://doi.org/10.1007/s12027-020-00625-7

Research ICT Africa. (2025, February 17). *The impact of social media and Generative AI on gender-based violence - Research ICT Africa*. https://researchictafrica.net/research/the-impact-of-social-media-and-generative-ai-on-gender-based-violence/

Safer Internet Day 2024 activities in Estonia. (n.d.). Better Internet for Kids. https://better-internet-for-kids.europa.eu/en/news/safer-internet-day-2024-activities-estonia

SaferInternet4kids. (n.d.). *SaferInternet4Kids | SaferInternet4Kids*. https://saferinternet4kids.gr/

Santi, P. (2024, May 1). Enfants et écrans : les constats qui ont nourri les préconisations de la commission nommée par Emmanuel Macron. *Le Monde.fr*. https://www.lemonde.fr/societe/article/2024/05/01/enfants-et-ecrans-les-constats-qui-ont-nourri-les-preconisations-de-la-commission-nommee-par-macron_6231003_3224.html

Sanusi, T. (2021, November 17). *Online Gender-Based Violence: What you need to know*. Global Citizen. http://globalcitizen.org/en/content/what-is-online-gender-based-violence-2/

Social media can change actions that drive gender-based violence | ISS Africa. (n.d.). ISS Africa. https://issafrica.org/iss-today/social-media-can-change-actions-that-drive-gender-based-violence

Tackling cyber violence against women and girls: The role of digital platforms. (2024, December 9). European Institute for Gender Equality. https://eige.europa.eu/publications-resources/publications/tackling-cyber-violence-against-women-and-girls-role-digital-platforms?language_content_entity=en

Targalt internetis. (n.d.). Targalt Internetis. https://www.targaltinternetis.ee/

Technology-Facilitated Gender-Based Violence: a growing threat. (n.d.). United Nations Population Fund. https://www.unfpa.org/TFGBV

The EU's Digital Services Act. (2022, October 27). European Commission. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

The role of technology in human trafficking. (n.d.). United Nations : Office on Drugs and Crime. https://www.unodc.org/unodc/en/human-trafficking/Webstories2021/the-role-of-technology-in-human-trafficking.html

Tomczyk, Ł. (2019). Skills in the area of digital safety as a key component of digital literacy among teachers. *Education and Information Technologies*, *25*(1), 471–486. https://doi.org/10.1007/s10639-019-09980-6

UN WOMEN. (2024). *REPOSITORY OF UN WOMEN'S WORK ON TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE (OCTOBER 2024)*. https://www.unwomen.org/sites/default/files/2024-10/repository-of-un-womens-work-on-technology-facilitated-gender-based-violence-en.pdf

University of Rhode Island, & Hughes, D. (2002). The Use of New Communications and Information Technologies for Sexual Exploitation of Women and Children. *Gender and Women's Studies Faculty Publications*. https://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1000&context=wms_facpubs

View of Digital Literacy: Education for Safe Internet usage. (n.d.). https://engagement.fkdp.or.id/index.php/engagement/article/view/1534/217

Westphal, V. (2024, April 12). *12% des adolescents déclarent se livrer à du cyberharcèlement*. Santé Mentale. https://www.santementale.fr/2024/04/un-jeune-sur-6-victime-de-cyberharcelement

What we know about the gender digital divide for girls: A literature review. (2023). In *UNICEF Gender and Innovation*.

https://www.unicef.org/eap/media/8311/file/What%20we%20know%20about%20the%20gender%20digital%20divide

Why Online Anonymity is Critical for Women - Women's Media Center. (n.d.). https://womensmediacenter.com/speech-project/why-online-anonymity-is-critical-for-women

Back to school in Greece with a focus on digital citizenship. (n.d.). Better Internet for Kids. https://better-internet-for-kids.europa.eu/en/news/back-school-greece-focus-digital-citizenship

Welens

Co-funded by
the European Union

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACE can be held responsible for them.