Welens

TOOLKIT SULLA VIOLENZA E SFRUTTAMENTO SESSUALE

MODULO 4

Tecnologia digitale e sinergie nella lotta alla violenza di genere

Cofinanziato dall'Unione europea

Progetto numero 2023-1-FR01-KA220-ADU-000165625

Nelle versioni inglese, spagnola, estone, russa e francese del presente Toolkit viene proposta una visione della prostituzione priva di agentività e dannosa in ogni sua forma, quella italiana e quella greca, invece, sono state sviluppate tenendo conto del dibattito in corso riguardo alla prostituzione, al sex work e allo sfruttamento sessuale e riflettono meglio la posizione del CESIE ETS e del gruppo di ricerca del Center for Security Studies, nonché quella proposta nel sistema legislativo greco.

Nello specifico, nei toolkit greco e italiano viene adoperata sempre l'espressione "sfruttamento sessuale nella prostituzione" per descrivere una forma di violenza sessuale che si verifica nel momento in cui un individuo sfrutta e approfitta, in maniera non consensuale e dannosa, del corpo di un altro soggetto a fini sessuali allo scopo di trarne un guadagno.

Entrambe le organizzazioni riconoscono l'importanza di operare una distinzione tra quanto descritto qui sopra e il lavoro sessuale o sex work inteso come uno scambio di servizi e prestazioni sessuali tra persone adulte consenzienti, in cambio di denaro, beni o un compenso. Tale scambio può assumere molte forme differenti e varia all'interno dei vari contesti culturali, ma non può prescindere dall'agentività dei soggetti coinvolti.

Pertanto, la parola "prostituzione", benché riconosciuta e utilizzata in ambito giuridico, non sarà utilizzata, poiché di tratta di un termine ombrello che non tiene conto delle suddette sfumature.

Indice

0. GLOSSARIO 3

1. Introduzione – Violenza di genere e tecnologie digitali: un'arma a doppio taglio 9

1.1. Le TIC come strumento di emancipazione 9

1.2. Le TIC come meccanismo di controllo e abuso 10

1.3. Impronta digitale: una mappa della vulnerabilità 11

2. Tipi di violenza di genere online 13

2.1. L'impatto dei social media 15

2.2. La duplice natura dell'anonimato 16

3. Sinergie intersettoriali e statali nella lotta alla violenza di genere 17

3.1. Quadri normativi dell'Unione Europea 19

3.2. Quadri nazionali 21

4. Sfruttamento digitale nella prostituzione e nella tratta transfrontaliera di esseri umani 31

4.1. Sfide della cooperazione internazionale 31

4.2. Correlazione con la migrazione 32

4.3. Educare le comunità alla sicurezza digitale 39

Cifre chiave: rischi online per le persone giovani 40

🧪 Esempi di attività da svolgere in classe 47

Come utilizzare queste risorse in modo efficace 47

4.4. L'impatto del settore privato 51

5. Conclusioni 54

6. Bibliografia 57

0. GLOSSARIO

Termine	Definizione
Discriminazione algoritmica	Fenomeno per cui i sistemi decisionali automatizzati producono risultati distorti o iniqui che svantaggiano individui o gruppi sulla base di caratteristiche quali razza, genere, età o status socioeconomico. Queste distorsioni derivano spesso da dati di addestramento distorti, da una progettazione imperfetta dei modelli o da disuguaglianze strutturali riflesse negli input. Si tratta di una questione fondamentale nelle discussioni sull'etica e la governance dell'intelligenza artificiale.
Tecnologie dell'informazione e della comunicazione (TIC)	Strumenti e piattaforme utilizzati per trasmettere e archiviare le informazioni e per accedervi, inclusi telefoni cellulari, servizi Internet e applicazioni digitali.
Violenza di genere (GBV)	Atti dannosi diretti contro individui in base al loro genere. Comprende abusi fisici, sessuali, psicologici ed economici, spesso rivolti a donne e ragazze.
Violenza di genere facilitata dalla tecnologia (TFGBV)	Qualsiasi forma di GBV amplificata, resa possibile o perpetrata attraverso tecnologie digitali quali social media, app mobili o forum online.
Tratta di esseri umani	Sfruttamento di individui attraverso la forza, la frode o la coercizione a fini di lavoro, sfruttamento sessuale o altri scopi. Questo fenomeno è sempre più facilitato dalle piattaforme digitali.

Sfruttamento online	Abuso o la manipolazione di individui tramite tecnologie Internet. Comprende lo sfruttamento sessuale, il ricatto, l'adescamento e la tratta.
Impronta digitale	Traccia di dati che gli individui lasciano quando utilizzano dispositivi digitali o piattaforme online. Comprende le registrazioni sia attive che passive delle attività.
Impronta digitale attiva	Dati generati intenzionalmente dagli utenti, come post, like, messaggi e upload, su siti web o piattaforme di social media.
Impronta digitale passiva	Dati raccolti senza l'input diretto dell'utente, tra cui tracciamento della posizione, cookie, metadati e abitudini di navigazione.
Pornografia *deepfake*	Contenuti sessuali manipolati digitalmente che raffigurano in modo falso un individuo, solitamente creati utilizzando l'intelligenza artificiale per imitarne le sembianze.
Schiavitù per debiti	Sistema di lavoro forzato in cui una persona impegna i propri servizi, o quelli di qualcuno sotto il suo controllo, come garanzia per un debito, che spesso porta allo sfruttamento quando i termini di rimborso sono manipolati o impossibili da soddisfare. Le vittime sono spesso intrappolate in cicli di povertà e servitù che si protraggono per generazioni.
Alfabetizzazione digitale	Capacità di interagire in modo critico e sicuro con le tecnologie digitali. Include la comprensione delle impostazioni sulla privacy, il riconoscimento delle minacce online e la navigazione responsabile sulle piattaforme.

Disinformazione	Creazione e diffusione deliberata di informazioni false o fuorvianti con l'intento di ingannare, manipolare la percezione o ottenere un vantaggio strategico.
Progettazione incentrata sulle persone sopravvissute	Approccio progettuale alla tecnologia che dà priorità alla sicurezza, all'autonomia e alle esigenze delle persone che hanno subito violenze o sfruttamento.
Intersezionalità	Quadro che riconosce come diversi aspetti dell'identità, quali il genere, la razza, la classe sociale e lo status migratorio, si intrecciano per plasmare esperienze di discriminazione e privilegio.
CEDAW (Convenzione sull'eliminazione di ogni forma di discriminazione della donna)	Trattato delle Nazioni Unite adottato nel 1979 che obbliga gli Stati a eliminare ogni forma di discriminazione nei confronti delle donne, compresa la violenza digitale, attraverso la Raccomandazione generale n. 35.
Convenzione di Istanbul	Trattato del Consiglio d'Europa incentrato sulla prevenzione e la lotta alla violenza contro le donne e alla violenza domestica, che riconosce lo stalking digitale e l'abuso psicologico.
Incels (celibi involontari)	Sottoculture online di uomini che ritengono di essere privati dell'accesso sessuale alle donne ed esprimono risentimento, odio o violenza nei confronti delle donne e degli uomini sessualmente attivi.
Disinformazione	Informazioni false o inesatte diffuse indipendentemente dall'intenzione di ingannare.

Convenzione di Budapest	Primo trattato internazionale sul crimine informatico che stabilisce gli standard legali per combattere i reati che coinvolgono i sistemi e le reti informatiche.
TFGBV (Violenza di genere facilitata dalla tecnologia)	Violenza commessa, agevolata o aggravata attraverso strumenti o piattaforme digitali, tra cui *cyberstalking, sextortion*, abuso basato su immagini e adescamento online.
Normativa sui servizi digitali (DSA)	Regolamento dell'Unione Europea (2022/2065) che impone alle piattaforme online l'obbligo di rimuovere i contenuti illegali, proteggere gli utenti e migliorare la trasparenza dei servizi digitali.
Inclusione digitale	Pratica che mira a garantire che tutti gli individui e le comunità, in particolare quelle emarginate o svantaggiate, abbiano accesso e la possibilità di utilizzare le tecnologie digitali. Pone l'accento non solo sulla connettività, ma anche sull'alfabetizzazione digitale, l'accessibilità economica e la disponibilità di servizi e contenuti inclusivi.
Regolamento generale sulla protezione dei dati (GDPR)	Legge dell'UE che disciplina la protezione dei dati e la privacy delle persone, compresa la protezione contro l'uso improprio dei dati personali sulle piattaforme digitali.
Geo-tagging	Processo che consiste nell'allegare dati di localizzazione geografica, come le coordinate di latitudine e longitudine, a media quali foto, video, siti web o messaggi di testo.
Disinformazione di genere	Forma di disinformazione che prende di mira le persone, in particolare le donne e le minoranze di genere, attraverso narrazioni, stereotipi e molestie basati sul genere. Combina informazioni false o

	fuorvianti con sessismo, misoginia e tropi di genere per minare la credibilità, mettere a tacere le voci e rafforzare le norme discriminatorie.
Condivisione di immagini non consensuale (NCII)	Conosciuta anche come "revenge porn", consiste nella distribuzione di contenuti sessualmente espliciti senza il consenso del soggetto, ed è considerata un reato dalla legge greca.
Diritto all'oblio	Principio della legge sulla protezione dei dati che conferisce alle persone la possibilità di richiedere la cancellazione dei dati personali quando questi non sono più necessari, sono inesatti o sono stati trattati in modo illecito.

INTRODUZIONE: Violenza di genere e tecnologie digitali: un’arma a doppio taglio

1. Introduzione – Violenza di genere e tecnologie digitali: un'arma a doppio taglio

L'avvento delle tecnologie digitali ha radicalmente riconfigurato il modo in cui le persone interagiscono, accedono alle informazioni e mobilitano il cambiamento sociale. Questa trasformazione non è stata priva di complessità, in particolare per le donne e le ragazze che navigano nella sfera digitale. Le tecnologie digitali, note anche come tecnologie dell'informazione e della comunicazione (TIC), hanno un enorme potenziale per emancipare le vittime di violenza di genere (GBV), in quanto consentono l'accesso a reti di sostegno, protezione legale e resistenza collettiva. Allo stesso tempo, però, questi strumenti possono essere utilizzati, e sempre più spesso lo sono, per perpetrare abusi, facilitare la tratta di esseri umani e rafforzare gli squilibri di potere.

Questo capitolo mira a svelare il duplice ruolo delle TIC nel favorire e combattere la violenza e lo sfruttamento di genere. Esamina inoltre il concetto di impronta digitale, rivelando come le tracce dei dati delle donne online possano essere sfruttate per la sicurezza o utilizzate come arma di controllo. A tal fine, il presente documento attinge da ricerche globali, casi di studio e sviluppi politici per fornire una panoramica completa del modo in cui gli ecosistemi digitali modellano la vulnerabilità e la resilienza.

1.1. Le TIC come strumento di emancipazione

Nella migliore delle ipotesi, le TIC offrono diverse possibilità di trasformazione per affrontare la violenza di genere. Le persone sopravvissute hanno infatti accesso a linee di assistenza digitali, servizi di messaggistica di emergenza e applicazioni mobili che facilitano la comunicazione discreta con i sistemi di supporto. Questi strumenti aggirano barriere quali l'isolamento geografico, lo stigma sociale e la paura di ritorsioni, soprattutto in contesti in cui l'accesso ai servizi fisici può essere pericoloso o impossibile.

Anche le piattaforme dei social media svolgono un ruolo sempre più importante nella difesa collettiva. Movimenti come #MeToo, #SayHerName e #NiUnaMenos dimostrano come gli spazi digitali siano diventati arene per la narrazione, la solidarietà e la mobilitazione. Tali campagne non solo sensibilizzano l'opinione pubblica, ma influenzano anche le riforme politiche e i cambiamenti culturali. Nelle regioni in cui le istituzioni tradizionali trascurano o

ignorano le preoccupazioni delle donne in materia di sicurezza, le TIC diventano una porta d'accesso alla visibilità e alla giustizia.

Le iniziative di inclusione digitale amplificano ulteriormente questi effetti. Ad esempio, le donne che vivono in zone remote o svantaggiate hanno accesso a assistenza legale a distanza, consulenza psicosociale e programmi di e-learning che sfidano l'isolamento storicamente utilizzato per zittirle o privarle di potere. Le piattaforme interattive consentono inoltre alle donne sopravvissute di documentare le loro esperienze, tenere traccia degli episodi di abuso e connettersi in modo anonimo con comunità di sostegno tra pari. La ricerca conferma che l'alfabetizzazione digitale è correlata a un aumento della ricerca di aiuto e a migliori risultati in termini di sicurezza.

1.2. Le TIC come meccanismo di controllo e abuso

Nonostante le promesse del progresso tecnologico, gli spazi digitali sono diventati anche terreno fertile per la misoginia e lo sfruttamento. **La violenza di genere facilitata dalla tecnologia (TFGBV)** comprende una serie di pratiche abusive: *cyberstalking*, molestie online, condivisione di immagini non consensuale ("revenge porn"), furto d'identità e minacce di danni fisici [5]. Queste violazioni sono amplificate dalla portata e dalla permanenza: i contenuti diffusi online possono raggiungere migliaia di persone in pochi istanti e rimanere accessibili a tempo indeterminato. **Internet è eterno:** una volta condiviso, il materiale dannoso può essere copiato, archiviato o ricaricato, il che rende quasi impossibile per le vittime rimuoverlo completamente.

Inoltre, le persone responsabili di questi reati sfruttano sempre più spesso strumenti di crittografia, navigazione anonima e dark web per sfuggire alle loro responsabilità. Ad esempio, nei casi di tratta di esseri umani, le piattaforme digitali vengono utilizzate per reclutare, adescare e controllare le vittime senza alcun contatto fisico. Le/i trafficanti pubblicizzano i loro servizi sui social media, utilizzano i dati di geolocalizzazione per tracciare i movimenti e sfruttano le app di incontri per attirare le donne in false relazioni che in seguito si trasformano in rapporti di sfruttamento.

Il costo psicologico della TFGBV non deve essere sottovalutato. Le vittime spesso riferiscono sentimenti di ipervigilanza, vergogna e impotenza, aggravati dalla difficoltà di rimuovere i contenuti dannosi o di identificare le persone responsabili degli abusi. Le forze dell'ordine spesso non dispongono delle capacità digitali o dell'autorità giurisdizionale necessarie per intervenire e, quindi, lasciano le vittime in uno stato di esposizione perpetua. Questo può provocare una nuova traumatizzazione, poiché le vittime sono costrette a rivivere il danno originale ogni volta che i contenuti abusivi riaffiorano online.

1.3. Impronta digitale: una mappa della vulnerabilità

Per comprendere a pieno lo sfruttamento online è essenziale conoscere il significato di impronta digitale, ovvero la traccia di dati generata dall'interazione di un individuo con le piattaforme digitali. Questa include impronte attive come post sui social media, acquisti online e messaggi, e impronte passive, tra cui metadati, tracciamento della posizione, cookie e cronologia di navigazione.

Sebbene le impronte digitali possano aiutare a raccogliere prove forensi contro le persone responsabili di reati, presentano anche rischi significativi. Ad esempio, la presenza digitale di una donna che fugge da relazioni abusive o ambienti coercitivi potrebbe essere sfruttata per localizzarla e molestarla. Le foto geotaggate, gli algoritmi predittivi e la raccolta di dati multipiattaforma rendono le persone sopravvissute vulnerabili non solo alle/ai responsabili di abusi noti, ma anche al marketing mirato, alla sorveglianza e persino alla discriminazione algoritmica.

Le giovani donne e le ragazze devono affrontare sfide specifiche. In particolare, gli studi dimostrano che le ragazze adolescenti tendono ad avere un minore controllo sulle impostazioni digitali, sono più propense a prendere in prestito dispositivi e spesso non hanno accesso a un'istruzione digitale completa. Inoltre, le ragazze provenienti da contesti emarginati, come le migranti, le giovani LGBTQ+ o quelle che vivono in condizioni di povertà, incontrano rischi aggravati a causa dell'esclusione sistematica e della limitata capacità di agire nel mondo digitale.

TIPI DI VIOLENZA DI GENERE ONLINE

2. Tipi di violenza di genere online

La violenza di genere facilitata dalla tecnologia, o violenza di genere online (GBV), è una forma di abuso sistemico che utilizza le tecnologie digitali per prendere di mira, zittire e controllare le persone in base al loro genere. Colpisce in modo sproporzionato le donne e le ragazze, rafforzando così gli squilibri di potere e perpetuando la discriminazione offline. La GBV online non è accidentale o isolata, ma fa parte di un continuum più ampio di violenza che abbraccia sia lo spazio fisico che quello virtuale. I suoi effetti sono reali, duraturi e spesso devastanti. Le forme più comuni includono:

- **Molestie online**: termine generico che si riferisce a qualsiasi comportamento indesiderato, aggressivo o minaccioso diretto a un individuo o a un gruppo attraverso piattaforme digitali. Comprende messaggi persistenti, insulti, minacce, molestie sessuali e attacchi coordinati. Le molestie online sono spesso di natura sessista, ovvero le donne e le ragazze subiscono abusi mirati alla loro identità e al loro aspetto.

- **Cyberbullismo:** molestie o umiliazioni ripetute e mirate attraverso le piattaforme digitali.

- ***Cyberstalking*:** monitoraggio o contatto persistente e indesiderato, spesso attuato tramite app di localizzazione o social media.

- ***Trolling*:** pubblicazione di commenti provocatori o denigratori per provocare o angosciare le vittime.

- **Attacchi di *cybermobbing* (*dogpiling*)**: molestie di gruppo coordinate o spontanee rivolte a un individuo online, spesso scatenate da un singolo post, opinione o identità. Questi attacchi coinvolgono in genere centinaia o migliaia di utenti che inviano minacce, insulti e messaggi disumanizzanti su più piattaforme, sopraffacendo il bersaglio e aumentando il danno emotivo e reputazionale. Gli individui sono spesso oggetto di *cybermobbing* dopo essersi espressi su questioni pubbliche.

- ***Hacking* e appropriazione di account (furto di identità online)**: accesso non autorizzato agli account online di qualcuno (social media, e-mail, archiviazione cloud) per rubare informazioni personali, impersonare la vittima o causare danni alla reputazione. Nei casi di violenza di genere, l'*hacking* viene spesso utilizzato per divulgare contenuti intimi, monitorare le comunicazioni o bloccare le persone dalle

loro piattaforme come forma di punizione o controllo.

- ***Doxxing*:** pubblicazione di informazioni private o identificative con l'intento di molestare o minacciare.

- **Abuso di *deepfake***: utilizzo dell'intelligenza artificiale per creare video o immagini falsi, spesso di natura sessuale, che ritraggono qualcuno senza il suo consenso. Questa forma di abuso basato sulle immagini può danneggiare gravemente la reputazione e la salute mentale.

- **Abuso basato sulle immagini:** condivisione di immagini o video intimi senza consenso (ad esempio, "revenge porn" o pornografia non consensuale).

- ***Sextortion*:** ricatto che comporta minacce di divulgazione di informazioni, foto o video a sfondo sessuale se le richieste non vengono soddisfatte.

- ***Catfishing***: creazione di un'identità online falsa per ingannare, spesso a scopo di manipolazione romantica, sfruttamento o abuso finanziario. Può portare a danni emotivi, ricatti o adescamento.

- **Adescamento**: costruzione di un rapporto di fiducia online con persone di minore età o individui vulnerabili a fini di sfruttamento o abuso sessuale. Le persone responsabili dell'adescamento spesso usano lusinghe, attenzioni o regali per manipolare le vittime.

- **Discorsi di incitamento all'odio e meme misogini:** diffusione di contenuti sessisti, violenti o discriminatori.

Queste forme di violenza possono sovrapporsi e spesso hanno gravi conseguenze psicologiche, sociali e persino economiche per le vittime.

* **Qual è la differenza tra bullo e hater online?**

Una/un **bullo** di solito prende di mira ripetutamente una persona specifica, spesso cercando di dominarla, intimidirla o umiliarla nel tempo. Una/un **hater,** invece, può pubblicare commenti dannosi, ostili o tossici senza necessariamente avere un legame personale o un interesse continuativo; spesso, l'azione dell'hater è spinta dal pregiudizio o dalla cultura del *trolling* piuttosto che da una vendetta personale. Sebbene entrambi i fenomeni siano dannosi, il bullismo è tendenzialmente più persistente e personale.

2.1. L'impatto dei social media

Gli spazi digitali sono il luogo in cui si svolge tutta la vita pubblica. Le piattaforme dei social media sono diventate fondamentali per connettersi, esprimersi e accedere alle informazioni. Tuttavia, hanno anche creato nuovi ambienti in cui può verificarsi la violenza di genere (GBV), spesso con una portata ampia e un impatto devastante. La GBV online non è solo un riflesso della disuguaglianza offline, ma anche un meccanismo che ne rafforza gli effetti attraverso la tecnologia.

- **Amplificazione degli abusi**

I social media possono amplificare rapidamente molestie, minacce e umiliazioni. Un singolo commento offensivo può essere ricondiviso, apprezzato o sommato ad altri, trasformando un attacco personale in un evento virale.

- **Anonimato e mancanza di responsabilità**

Sebbene l'anonimato possa proteggere gli utenti vulnerabili, consente anche di perpetrare molestie senza temere conseguenze. I profili falsi e i sistemi di moderazione deboli contribuiscono a creare una cultura in cui le minacce e gli abusi raramente vengono affrontati in modo efficace.

- **Normalizzazione dei contenuti dannosi**

Battute sessiste, cultura dello stupro e meme misogini spesso circolano ampiamente e vengono liquidati come "semplice umorismo" o "libertà di espressione". Questo normalizza la violenza, rafforza gli stereotipi di genere e scoraggia le vittime dal denunciare.

    - **Comunità *incel***: le sottoculture online, come gli *incel* (celibi involontari), sono un fattore chiave dei contenuti misogini e dei discorsi di odio di genere. I forum *incel* e gli spazi dei social media normalizzano l'ostilità verso le donne, promuovono stereotipi dannosi e talvolta glorificano la violenza sessuale.

- **Sorveglianza e controllo**

I social media possono essere utilizzati per monitorare, perseguitare o controllare il comportamento di qualcuno, soprattutto nelle relazioni abusive. Funzionalità come il *geotagging*, i messaggi “visualizzati” o le foto taggate possono essere utilizzati come armi per tracciare e intimidire.

- **Silenzio, autocensura e paura di parlare**

Di fronte a continue molestie, molte donne e persone emarginate limitano ciò che condividono, abbandonano le piattaforme o evitano di partecipare al dibattito pubblico. Altre scelgono di non parlare affatto delle esperienze di violenza di genere facilitata dalla tecnologia perché temono il bullismo, l'umiliazione, l'attribuzione di colpa o la mancata

credibilità. Ciò porta al silenzio delle voci e delle prospettive critiche e rafforza la percezione che gli spazi online non siano sicuri per le donne.

- **Diffusione di disinformazione e disinformazione di genere**

I social media sono uno strumento potente per diffondere informazioni false, compresi stereotipi di genere dannosi o campagne di disinformazione mirate contro attiviste, giornaliste o politiche, con l'obiettivo di minarne la credibilità e la sicurezza.

2.2. La duplice natura dell'anonimato

Nel contesto della violenza di genere online, l'anonimato gioca un ruolo complesso e spesso controverso. Può infatti avere effetti sia abilitanti che protettivi, a seconda della prospettiva e del contesto.

Modi in cui l'anonimato favorisce le persone responsabili di abusi:

- Riduzione delle responsabilità**:** la possibilità di nascondere la propria identità online può incoraggiare le persone a compiere comportamenti abusivi, come molestie, minacce e stalking, senza temere conseguenze nel mondo reale.
- Escalation degli abusi**:** l'anonimato può facilitare forme di abuso più aggressive o persistenti, poiché fa sentire al riparo dall'individuazione e dalla punizione.
- Difficoltà nell'applicazione della legge: le forze dell'ordine e le autorità che moderano le piattaforme spesso incontrano difficoltà nell'identificare e perseguire le persone responsabili degli abusi la cui identità è nascosta.

Modi in cui l'anonimato protegge le vittime:

- Sicurezza per le persone sopravvissute**:** per le vittime e le persone sopravvissute alla violenza di genere, l'anonimato può essere fondamentale per cercare sostegno, condividere esperienze o partecipare ad attività di advocacy senza rischiare ritorsioni o ulteriori danni.
- Privacy per i gruppi vulnerabili**:** le donne, le/gli attiviste/i e coloro che vivono in contesti oppressivi possono fare affidamento su identità anonime per esprimersi in modo sicuro e accedere alle risorse.
- Emancipazione**:** l'anonimato consente ad alcuni utenti di partecipare a spazi online che altrimenti eviterebbero per paura di essere presi di mira o di subire discriminazioni.

SINERGIE INTERSETTORIALI E STATALI NELLA LOTTA ALLA VIOLENZA DI GENERE

3. Sinergie intersettoriali e statali nella lotta alla violenza di genere

La violenza di genere (GBV) non è solo un trauma personale o isolato, ma una crisi globale profondamente radicata e costante che si ripercuote su ogni strato della società. Che si tratti della pressione sui sistemi sanitari, degli effetti a catena sui sistemi educativi o del costo per la crescita economica, la GBV non lascia indenne nessun settore, ancor più quando le sue forme online stanno penetrando nella vita delle donne ovunque esse risiedano, in ogni nazione e continente. Pertanto, affrontare la GBV online richiede più degli sforzi dei singoli Paesi: una collaborazione autentica e sostenuta tra governi, comunità e istituzioni, guidata dalla responsabilità condivisa e dalla fiducia reciproca.

La maggior parte degli Stati riconosce ormai la violenza di genere come una violazione dei diritti umani. Strumenti giuridici come la Convenzione di Istanbul e la CEDAW hanno spinto i governi ad adottare leggi e strategie nazionali. Tuttavia, il quadro normativo non è sufficiente; molti Paesi falliscono proprio nell'attuazione. Alcuni Paesi non hanno ancora adottato approcci incentrati sulle vittime o non riescono ad allocare fondi adeguati, mentre altri hanno leggi sulla carta (probabilmente per rispettare i quadri normativi e le iniziative internazionali o regionali), ma non dispongono di meccanismi di applicazione adeguati.

Dato che nessun settore può affrontare da solo la violenza di genere online, la collaborazione intersettoriale è fondamentale. I servizi sanitari, le forze dell'ordine, l'istruzione e il welfare sociale dovrebbero collaborare in modo complementare per ottenere risultati efficaci. Ad esempio, gli ospedali hanno bisogno di protocolli per identificare gli abusi e indirizzare le vittime; la polizia deve essere formata per gestire i casi con sensibilità e tempestività; le scuole dovrebbero insegnare il consenso e il rispetto sin dalle prime fasi. Colmando queste lacune, i sistemi di riferimento integrati e programmi di formazione congiunti possono avere un impatto tangibile.

La cooperazione internazionale è sempre più cruciale, poiché la violenza online non ha limiti né è contenuta entro i confini di un singolo Paese. La tratta di esseri umani, gli abusi online e la migrazione forzata hanno tutti dimensioni transfrontaliere. Entra in gioco la cooperazione internazionale: gli organismi delle Nazioni Unite, le alleanze regionali e le ONG svolgono un ruolo chiave nella condivisione dei dati, nel finanziamento dei programmi e nella responsabilizzazione degli Stati. Gli Obiettivi di Sviluppo Sostenibile (in particolare l'SDG5) hanno contribuito ad allineare gli sforzi globali, ma occorre fare di più per garantire che gli impegni si traducano in azioni concrete.

In sostanza, la lotta contro la violenza di genere online è complessa. Non si tratta solo di punire le persone responsabili dopo che il reato è stato commesso, ma anche di cambiare i sistemi alla loro base. A tal fine, gli Stati devono andare oltre la retorica, i diversi settori devono evitare di lavorare in modo isolato e gli attori internazionali devono continuare a premere per una maggiore responsabilizzazione.

3.1. Quadri normativi dell'Unione Europea

Esistono leggi a livello europeo e meccanismi pertinenti sulle piattaforme online, compresi i siti web pornografici, per proteggere gli utenti, in particolare le donne e le persone di minore età, e per segnalare e/o richiedere la rimozione di contenuti.

In base alle leggi dell'UE sulle piattaforme online e sui siti web pornografici, il regolamento *Digital Services Act* (DSA), pienamente applicabile dal 17 febbraio 2024, si applica a tutte le piattaforme. In particolare, le piattaforme online di grandi dimensioni (VLOP) come Pornhub, Stripchat e XVideos devono:

- Effettuare delle valutazioni dei rischi non solo in relazione a possibili contenuti illegali, ma anche specificamente in relazione alla violenza di genere e alla sicurezza delle persone di minore età online.
- Implementare sistemi di verifica dell'età in modo da bloccare l'accesso dei minori ai siti che contengono contenuti pornografici.
- Rimuovere immediatamente i contenuti segnalati o ritenuti illegali o non consensuali.
- Mantenere la trasparenza e la responsabilità sottoponendosi a verifiche indipendenti.
- Essere sempre soggette a controlli sia per quanto riguarda la parzialità che i danni.

Il mancato rispetto di uno qualsiasi dei punti sopra menzionati può comportare multe fino al 6% del fatturato annuo globale o addirittura divieti a livello europeo.

Inoltre, per proteggere le donne online, la direttiva sulla cyberviolenza del 2024, che dovrebbe essere attuata entro il 2027, include la criminalizzazione del *revenge porn*, del *cyberstalking*, delle molestie sessuali online e dei *deepfake* non consensuali. A tal fine, i siti web devono rimuovere le immagini intime o manipolate che vengono pubblicate online senza consenso. Attraverso una direttiva a livello europeo, le vittime avranno accesso alla giustizia e ai servizi di assistenza in tutta l'UE.

La segnalazione di contenuti online dannosi o illegali può essere effettuata in vari modi:

- Direttamente alle piattaforme pertinenti utilizzando gli appositi strumenti conformi al DSA.
- Attraverso gruppi della società civile designati esplicitamente dall'UE per segnalare i casi più gravi.
- Ai coordinatori nazionali dei servizi digitali (DSC), organismi istituiti in ciascuno Stato membro dell'UE per vigilare sulla conformità dei siti web al DSA.
- Per i casi più complessi, i reclami possono essere presentati direttamente tramite il portale della strategia digitale dell'UE.

Di seguito si illustra la procedura di segnalazione di un reato online:

FASE 1: identifica il contenuto

↓

Specifica il contenuto dannoso o illegale e la sua posizione (URL)

↓

FASE 2: spiega la violazione

↓

Descrivi in che modo il contenuto viola il DSA o il GDPR

↓

FASE 3: fornisci dettagli

↓

Spiega la tua relazione con il contenuto e fornisci qualsiasi prova a sostegno

↓

FASE 4: richiedi la rimozione

↓

Chiedi la rimozione immediata e una risposta tempestiva

3.2. Quadri nazionali

FRANCIA

La Francia ha implementato un quadro giuridico completo per proteggere le persone di minore età dall'esposizione a contenuti pornografici e dannosi online. Il Paese combina il diritto penale, la regolamentazione digitale e rigorosi meccanismi di applicazione per garantire la conformità, in particolare a seguito della recente legge sui servizi digitali (DSA) dell'UE.

Quadro giuridico e politico

- **Il codice penale francese (articolo 227-24)** vieta l'accessibilità dei contenuti pornografici per le persone di minore età. La legge si applica sia alla distribuzione fisica che a quella online. Gli operatori non conformi rischiano **fino a 3 anni di reclusione e 75.000 euro di multa**.
- **La legge n. (2024) -449** (SREN - Legge per la sicurezza e la regolamentazione dello spazio digitale), promulgata nel **maggio 2024**, impone ai siti web con contenuti pornografici di implementare **sistemi di verifica dell'età affidabili**. Questa legge si applica a tutti i siti accessibili dalla Francia, compresi quelli gestiti all'estero.
- **L'ARCOM**, l'autorità nazionale di regolamentazione, è stata incaricata di monitorare e far rispettare questi obblighi. Può emettere avvertimenti formali, infliggere multe, richiedere audit e ordinare restrizioni di accesso o **il blocco dei siti web non conformi**.
- (**ARCOM** – Autorità di regolamentazione per la comunicazione audiovisiva e digitale)

Misure di applicazione e verifica dell'età

- **Nell'ottobre 2024**, l'ARCOM ha pubblicato le **linee guida tecniche** per la verifica dell'età conforme:
    - Utilizzo di **sistemi a doppio anonimato**, che garantiscono l'assenza di collegamenti tra l'identità dell'utente e il suo comportamento di navigazione.
    - **Verifica** indipendente **da parte di terzi**, separata dalla piattaforma stessa.
    - **Nessuna memorizzazione di dati personali** o identificativi.
- Fino all'inizio del 2025 è stato consentito un **meccanismo transitorio** che prevedeva la verifica temporanea della carta di credito. Attualmente, i siti devono passare alla piena conformità utilizzando sistemi di verifica anonimi certificati.
- **All'inizio del 2025**, l'ARCOM ha pubblicato un elenco di **17 siti web per persone adulte** (tra cui Pornhub, RedTube e altri) soggetti a conformità obbligatoria. A metà del 2025, **diversi siti sono stati bloccati o rimossi dall'elenco** a causa della mancata implementazione di controlli adeguati, come approvato dal tribunale.
- Le multe previste dalla legge SREN possono raggiungere **i 150.000 euro o fino al 2% del fatturato annuo globale**, con misure progressive per i recidivi.

Come segnalare contenuti illegali o richiederne la rimozione

Caso	**Piattaforma/Autorità**	**Descrizione**
Contenuti illegali (ad es. materiale pedopornografico, adescamento di minori, contenuti terroristici)	**PHAROS**	Piattaforma nazionale per la segnalazione di reati online gestita dal Ministero dell'Interno. Accetta segnalazioni anonime. www.internet-signalement.gouv.fr
Cyberbullismo, *revenge porn*, esposizione indesiderata a contenuti per persone adulte, *sextortion*	**3018 (Associazione e-Enfance)**	Linea di assistenza dedicata a persone di minore età e genitori. Segnalazione rapida a piattaforme come TikTok, YouTube e Instagram. Gratuita, riservata, disponibile tramite telefono, SMS, chat o app. www.3018.fr

Esposizione dei dati personali, diritto all'oblio	**CNIL** (Autorità francese per la protezione dei dati)	Gestisce le richieste relative al GDPR per la cancellazione dei dati o la rimozione dai motori di ricerca. www.cnil.fr

- Alla fine del 2024, **e-Enfance è stata ufficialmente designata come "segnalatore affidabile" dall'ARCOM**, il che significa che le principali piattaforme danno la priorità alle segnalazioni provenienti dal 3018.

Il quadro giuridico e istituzionale francese attribuisce grande importanza **alla protezione dei minori dalla pornografia online e dagli abusi digitali**. Le nuove leggi (SREN) impongono requisiti di verifica dell'età e conferiscono all'ARCOM il potere di farli rispettare. Il diritto penale (articolo 227-24) punisce l'esposizione delle persone di minore età a tali contenuti. I sistemi di segnalazione, come **PHAROS** (per i contenuti illegali) e **3018** (per il supporto e la rimozione rapida), offrono agli utenti efficaci vie di protezione. La Francia combina quindi **una legislazione rigorosa, un'applicazione attiva e meccanismi di segnalazione di facile utilizzo,** in linea con i suoi obblighi UE ai sensi del ***Digital Services Act*** **(DSA).**

ITALIA

In Italia esistono normative specifiche che disciplinano la protezione dei dati personali e stabiliscono misure di sicurezza obbligatorie da adottare. Una delle principali normative in questo settore è il Regolamento generale sulla protezione dei dati (GDPR), entrato in vigore nel 2018. Tale regolamento stabilisce una serie di principi e obblighi che le organizzazioni devono rispettare per garantire la protezione dei dati personali. Tra le misure di sicurezza obbligatorie previste dal GDPR vi è l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tra cui l'uso della crittografia, l'implementazione di procedure di backup e il controllo dell'accesso ai dati. Oltre al GDPR, l'Italia dispone di altre normative che disciplinano la protezione dei dati personali. Ad esempio, il Codice in materia di protezione dei dati personali (Decreto Legislativo 196/2003) stabilisce le misure di sicurezza che le organizzazioni devono adottare per proteggere i dati personali. Tra queste misure vi è l'obbligo di adottare misure tecniche e organizzative adeguate a garantire la sicurezza dei dati personali e per prevenirne la perdita, la distruzione o l'accesso non autorizzato (Diritto.net, 2023b).

Per quanto riguarda la pornografia, in Italia è legale guardare video pornografici su Internet, cioè in streaming, così come scaricarli. Tuttavia, nel caso dei download, è necessario assicurarsi che il contenuto sia di libero utilizzo, cioè non protetto da copyright, altrimenti si può incorrere in una sanzione diversa per violazione del copyright. La pornografia infantile, cioè la pornografia che coinvolge le persone di minore età, è invece una questione a parte.

In questo caso, sebbene la semplice visione di tali video su Internet non sia punibile, lo è invece il possesso o la distribuzione del materiale (La Legge Per Tutti, 2015). Il codice penale italiano, all'articolo 600-bis, definisce la pornografia infantile come la produzione, il possesso, la distribuzione e il trasferimento di materiale pornografico che coinvolge persone di minore età inferiore ai 18 anni. Questo reato è considerato particolarmente grave ed è perseguito attivamente dalle autorità di polizia. Per combattere efficacemente la pornografia infantile e i reati online contro le persone di minore età sono state adottate diverse misure legislative. Tra queste, la legge n. 38/2006 ha introdotto il reato di adescamento di minori tramite Internet, punendo chiunque si avvicini a un minore con l'intento di commettere reati sessuali (Diritto.net, 2023a). Inoltre, nel 2022, l'accesso intenzionale a siti web contenenti materiale pedopornografico è stato definito come un reato penale, punibile con una sanzione non inferiore a 1000 euro e con la reclusione fino a 2 anni (Agenda Digitale, 2022).

Per **segnalare** un sito web illegale in Italia, la denuncia deve essere presentata di persona alla polizia postale o ad altre forze dell'ordine. Tuttavia, è possibile avviare la procedura online inviando i propri dati personali e i dettagli del reato sul sito web della Polizia di Stato. Dopo l'invio, si riceve una ricevuta elettronica e un numero di protocollo da seguire di persona. Questa procedura online non sostituisce la denuncia ufficiale, ma funge da bozza preparatoria. La denuncia acquista validità legale solo una volta firmata fisicamente davanti a un agente di polizia. Pertanto, il modulo online aiuta a preparare e organizzare accuratamente la denuncia, ma la denuncia formale definitiva richiede una visita di persona alle forze dell'ordine.

GRECIA

In Grecia esistono diversi modi per segnalare contenuti e/o richiedere assistenza, come descritto di seguito:

- **Contenuti illegali o dannosi (ad esempio, abusi su persone di minore età, adescamento, incitamento all'odio):**
    - Segnalazione tramite SafeLine.gr
    - Contattare la Divisione Crimini Informatici tramite la linea telefonica 11188 o l'e-mail
- **Pornografia vendicativa o contenuti espliciti non consensuali:**
    - Presentare una denuncia alla polizia
- **Protezione delle persone di minore età e controlli parentali per fornire assistenza in casi di adescamento o richiesta di foto personali a persone di minore età:**

    - Parco.gov.gr per guide e strumenti

- **La rimozione dei contenuti (ad esempio, risultati di ricerca obsoleti o dannosi) è valida in tutti i Paesi:**
    - Invio di una richiesta tramite il Centro assistenza legale di Google o il modulo "Diritto all'oblio".

La tabella seguente presenta le aree tematiche, i quadri giuridici di riferimento e l'autorità greca responsabile.

Area	**Quadro giuridico/politico**	**Autorità responsabile**
Piattaforme online e servizi di intermediazione	La legge 5099/2024, che attua il *Digital Services Act* (DSA) dell'UE, disciplina i contenuti illegali, la trasparenza e la protezione degli utenti	Commissione ellenica per le telecomunicazioni e le poste (HTPC), Consiglio nazionale per la radio e la televisione (NCRT), Autorità ellenica per la protezione dei dati (HDPA)
Siti web pornografici e *revenge porn*	L'articolo 346 del codice penale (legge 4947/2022) criminalizza la distribuzione non consensuale di contenuti intimi	Divisione Crimini Informatici della Polizia Ellenica, Procura
Protezione delle persone di minore età online	Strategia nazionale per la protezione delle persone di minore età dalla dipendenza da Internet; include controlli parentali, l'app Kids Wallet e la verifica dell'età	Ministero della Governance Digitale, Ministero dell'Istruzione, Divisione Crimini Informatici della Polizia Ellenica
Segnalazione di contenuti illegali (ad es. CSAM, incitamento	SafeLine.gr (Centro greco per un Internet più sicuro); membro INHOPE; gestisce le segnalazioni di contenuti illegali	Hotline SafeLine, Divisione Crimini Informatici della Polizia Ellenica

all'odio, adescamento)		
Richiesta di rimozione di contenuti (diritto all'oblio, contenuti dannosi)	GDPR e leggi nazionali sulla privacy; moduli legali di Google per la rimozione; SafeLine per contenuti illegali	Centro assistenza legale di Google, SafeLine.gr, Autorità ellenica per la protezione dei dati

ESTONIA

In **Estonia**, il quadro giuridico che disciplina le piattaforme online, i siti web pornografici e la protezione degli utenti, in particolare delle persone di minore età, è integrato in leggi e politiche più ampie sulla protezione, sui diritti dei consumatori e sulla sicurezza digitale, piuttosto che in una singola legge dedicata.

Area	**Quadro giuridico/politico**	**Autorità responsabile**
Protezione delle persone di minore età da contenuti violenti/crudeli	Legge sulla protezione dei minori, paragrafo 25	Ministero degli Affari Sociali, Agenzie per la protezione dei minori
Restrizioni pubblicitarie rivolte alle persone di minore età	Legge sulla pubblicità	Autorità per la tutela dei consumatori e la regolamentazione tecnica
Restrizioni sui contenuti che incitano all'odio/alla violenza	Poteri dell'Autorità per la tutela dei consumatori e la regolamentazione tecnica	Autorità per la tutela dei consumatori e la regolamentazione tecnica
Prevenzione degli abusi sessuali sulle persone di minore età online	Piano di sviluppo della sicurezza interna 2025-2028	Ministero dell'Interno
Attuazione della legge sui	Attuazione nazionale in	Autorità per la protezione dei

servizi digitali dell'UE	corso	consumatori e la regolamentazione tecnica
Sicurezza dei dati e protezione degli utenti	Sistema di identificazione elettronica, tecnologia blockchain	Ministero della Giustizia e degli Affari digitali, RIA (Autorità per i sistemi informativi)

Sebbene non esista una legge estone specifica che regoli esclusivamente i siti web pornografici, il DSA e le leggi nazionali impongono alle piattaforme di impedire l'accesso delle persone di minore età a contenuti dannosi. La legge sui servizi mediatici regola i servizi mediatici audiovisivi, compresi i contenuti on demand, richiedendo la registrazione e il rispetto degli standard relativi ai contenuti. Questi quadri normativi implicano la verifica dell'età e restrizioni sui contenuti dannosi per le persone di minore età.

Come segnalare, richiedere la rimozione dei contenuti e chiedere aiuto?

- Coordinatore estone dei servizi digitali: ai sensi della legge dell'UE sui servizi digitali, l'Autorità estone per la protezione dei consumatori e la regolamentazione tecnica funge da coordinatore per i reclami relativi a contenuti illegali sulle grandi piattaforme online. È possibile presentare reclami se le piattaforme non rimuovono contenuti dannosi o illegali, compresa la violenza di genere online.

- Denuncia alla polizia: le vittime di violenza di genere online possono denunciare alla polizia estone reati quali *cyberstalking*, minacce o distribuzione di immagini non consensuali. Le forze dell'ordine possono indagare e intraprendere azioni legali.

Dove chiedere aiuto:

- Linea di assistenza alle vittime (116006): disponibile 24 ore su 24, 7 giorni su 7, in estone, inglese e russo, questa linea di assistenza gratuita fornisce consulenza riservata, sostegno emotivo e orientamento alle vittime di violenza, compresa la violenza di genere online e la violenza sessuale. Offre inoltre informazioni sui diritti legali e sui servizi disponibili.

- Centri di crisi per la violenza sessuale: centri specializzati forniscono assistenza gratuita e olistica alle vittime di violenza sessuale, comprese quelle colpite da molestie o abusi sessuali online.

- Campagna e sito web “Notice. Intervene. Help.” : l'Ente previdenziale sta conducendo una campagna incentrata sulla prevenzione delle molestie sessuali, comprese

quelle online. Il sito web www.palunabi.ee/ooelu offre consigli pratici alle vittime e ai testimoni su come distinguere le molestie e su come intervenire in modo sicuro.

GUYANA

La Guyana ha compiuto notevoli progressi nella creazione di un modello di risposta interconnesso che riflette un approccio multidimensionale.

Quadri politici

Il panorama legislativo e politico della Guyana si è evoluto per fornire protezioni e meccanismi di responsabilità più forti:

- **Legge sulla violenza familiare (2024)**: una riforma storica che integra rimedi sia penali che civili, conferendo ai tribunali e alla polizia il potere di intervenire nei casi di violenza domestica.
- **Legge sui reati sessuali (2010, modificata nel 2013**) e Legge sulla violenza domestica (1996, aggiornata nel 2015): queste leggi costituiscono la spina dorsale della protezione giuridica per le vittime.
- **Politica nazionale per l'uguaglianza di genere e l'inclusione sociale (2018)**: promuove la riforma giuridica, l'assistenza alle vittime e l'educazione pubblica per eliminare la violenza e la discriminazione.

Inoltre, la risposta della Guyana alla violenza di genere si basa su un coordinamento multisettoriale:

- Il **Ministero dei servizi sociali e della sicurezza sociale** guida l'attuazione attraverso l'Unità per la politica sui reati sessuali e la violenza domestica.
- La **polizia della Guyana** ha ora ampliato la propria autorità per intervenire nei casi privati di violenza di genere, compreso l'arresto e l'allontanamento delle persone responsabili.
- Il coinvolgimento del **settore sanitario** comprende simposi medici e formazione sull'assistenza informata sul trauma per le/i professioniste/i.
- La **Community Advocate Network (CAN)** mobilita le/i leader di base per sostenere le vittime e sensibilizzare l'opinione pubblica.
- La **hotline 914** offre un supporto rapido e riservato alle vittime in tutto il Paese.

Le partnership globali della Guyana riguardano quanto segue:

- **Iniziativa Spotlight (UE e ONU):** il modello della Guyana, nato da questa iniziativa, è riconosciuto come leader regionale nella risposta alla violenza di genere. Canalizza finanziamenti, supporto tecnico e strumenti di monitoraggio verso i programmi locali.
- **Quadri PANCAP e CARICOM**: promuovono il dialogo regionale, la condivisione dei dati e l'armonizzazione delle politiche tra gli Stati caraibici.
- **Strategia di Montevideo e sinergia Pechino +25:** allinea gli sforzi della Guyana agli obiettivi globali di uguaglianza di genere, compresa la protezione delle donne indigene e delle sopravvissute alla tratta.

SFRUTTAMENTO DIGITALE NELLA PROSTITUZIONE E NELLA TRATTA TRANSFRONTALIERA DI ESSERI UMANI

4. Sfruttamento digitale nella prostituzione e nella tratta transfrontaliera di esseri umani

La vulnerabilità delle donne allo sfruttamento sessuale digitale è radicata anche nelle disuguaglianze strutturali. L'accesso limitato all'istruzione, gli alti tassi di disoccupazione, la povertà e le conseguenti scarse opportunità economiche spesso limitano le scelte delle donne, spingendo alcune verso la produzione di contenuti sessuali online (come pornografia, sesso online o piattaforme di escort) come una delle poche fonti di reddito disponibili. Questi rischi sono accentuati per le donne che emigrano per lavoro o sono sfollate a causa di conflitti o crisi ambientali, poiché spesso devono affrontare precarietà giuridica, barriere linguistiche e assenza di reti di sostegno. La mancanza di risorse e di educazione digitale o sessuale aumenta ulteriormente la loro esposizione a reclutamenti ingannevoli e coercizioni. Comprendere questi fattori sistemici è essenziale per affrontare il modo in cui le piattaforme digitali diventano luoghi di sfruttamento piuttosto che di emancipazione.

4.1. Sfide della cooperazione internazionale

Sebbene la cooperazione internazionale e transfrontaliera nella lotta alla violenza di genere online e allo sfruttamento digitale delle donne sia della massima importanza, esistono numerose perplessità e lacune circa, ad esempio, i diversi quadri giuridici, i limiti e gli ostacoli giurisdizionali, le politiche di estradizione, l'interoperabilità delle banche dati e i tempi di risposta lenti dovuti ai processi interni e alla burocrazia.

- **Barriere legali e giurisdizionali**: poiché anche le definizioni giuridiche differiscono, i Paesi possono interpretare in modo diverso concetti come la violenza informatica, il consenso e lo sfruttamento digitale. Un atto considerato criminale in una giurisdizione potrebbe non esistere (ancora) nel quadro giuridico di un altro Paese, cosicché l'atto in questione rimane non regolamentato e senza restrizioni.

- **Ambiguità giuridica transfrontaliera**: poiché le persone responsabili dei reati operano spesso a livello internazionale, determinare quale Paese abbia l'autorità di perseguire un determinato atto criminale potrebbe richiedere diverso tempo. Le avvocatesse e gli avvocati difensori sfruttano questa situazione a loro vantaggio, inventando scappatoie al solo scopo di ritardare la giustizia.

- **Limiti all'estradizione**: ad oggi, molti trattati internazionali non affrontano ancora il tema della criminalità informatica. Pertanto, anche se esistono procedure di estradizione, sono necessari nuovi trattati o protocolli aggiuntivi affinché le vittime possano ottenere un ricorso legale.

- **Lacune e disparità operative e amministrative delle forze dell'ordine**: non tutti i Paesi dispongono delle stesse infrastrutture, formazione, capacità o competenze per affrontare la violenza di genere facilitata dalla tecnologia.

- **Difficoltà nella raccolta di prove digitali**: raccogliere prove digitali utilizzabili in procedimenti giudiziari in diverse giurisdizioni è complesso sia dal punto di vista tecnico che giuridico.

- **Politiche e coordinamento frammentati**: la mancanza di protocolli unificati e di standard globali per affrontare la violenza di genere online rende gli sforzi internazionali incoerenti e spesso inefficaci. Questi fattori dipendono principalmente dalle lacune nei dati; senza pratiche armonizzate di raccolta dei dati, le procedure richiedono più tempo, impegno e risorse.

- **Società civile sottoutilizzata**: le ONG e le organizzazioni di base sono spesso in prima linea nel sostegno e nella difesa delle vittime, eppure raramente vengono integrate nei meccanismi formali di coordinamento internazionale o nelle sessioni di consultazione.

- **Responsabilità, trasparenza e conformità complesse delle piattaforme**: esistono servizi, siti web e applicazioni che possono operare al di fuori della portata delle leggi nazionali e possono opporsi alle richieste di rimozione di contenuti dannosi o di condivisione di dati degli utenti/possibili responsabili di crimini. In questo caso, ovviamente, riappare il dilemma tra privacy e responsabilità; la crittografia e l'anonimato sono sicuramente essenziali per la sicurezza delle donne online, ma consentono anche alle persone responsabili di agire e complicano le indagini.

- **Mancanza di volontà politica**: alcuni Paesi non riconoscono a pieno la gravità della violenza e dello sfruttamento di genere online e, quindi, non sono inclini a partecipare attivamente alle iniziative transfrontaliere.

4.2. Correlazione con la migrazione

I conflitti armati, i cambiamenti climatici (perdita di produttività, catastrofi, aumento dei prezzi dei generi alimentari), la povertà e le disuguaglianze sociali sono tutte cause alla base della migrazione ed espongono le persone al rischio di tratta e sfruttamento. Le persone migranti sono considerate particolarmente vulnerabili allo sfruttamento sessuale

e alla tratta a causa di una combinazione di **fattori di rischio strutturali, sociali e personali** che le/i trafficanti sfruttano attivamente. Questi includono la precarietà giuridica ed economica, come lo status giuridico irregolare o incerto, la vulnerabilità finanziaria e, in alcuni casi, la schiavitù per debiti. Spesso le persone migranti non conoscono la **lingua, i diritti e le tutele giuridiche** del Paese ospitante**,** il che può impedire loro di cercare aiuto. La mancanza di accesso a informazioni accurate rende più facile per le/i trafficanti ingannare queste persone sulle condizioni di lavoro o sui requisiti legali. Inoltre, spesso le persone migranti non dispongono di solide **reti sociali e familiari** nel Paese ospitante, il che le rende vulnerabili allo sfruttamento da parte di reclutatrici/reclutatori, datrici/datori di lavoro o intermediari. Le persone migranti che cercano lavoro online o attraverso gruppi informali sui social media sono spesso oggetto di **offerte fasulle** (ad esempio, lavoro domestico, ospitalità, modellismo) che si trasformano in situazioni di tratta.

A livello globale, il numero delle vittime della tratta è in aumento dall'inizio della pandemia di COVID-19 e si registrano sempre più casi di vittime di minore età. Le ragazze e i ragazzi mostrano modelli di sfruttamento diversi: la maggior parte delle ragazze vittime individuate (60%) è stata trafficata a fini di sfruttamento sessuale, mentre questa percentuale è solo dell'8% per i ragazzi. Lo stesso vale per le donne, per le quali lo sfruttamento sessuale rappresenta il 66%. Questa forma di tratta comprende una varietà di tipi di sfruttamento, dalla prostituzione forzata delle persone adulte e lo sfruttamento sessuale delle bambine e dei bambini alla schiavitù sessuale. Per quanto riguarda lo sfruttamento digitale, gli esempi di casi giudiziari includono casi di bambine e bambini sfruttati per produrre materiale pedopornografico, spettacoli in webcam e cybersesso (UNODC, *Global Report on Trafficking in Persons* ; dati e analisi globali).

Le piattaforme digitali sono diventate fondamentali per facilitare la prostituzione e la tratta. In alcune regioni, gli account dei social media sono associati a oltre il 60% dei casi di tratta identificati e il 77% delle/dei trafficanti prende di mira le bambine e i bambini utilizzando i social media e altri strumenti online (https://endexploits.com/statistics.html).

Le/i trafficanti utilizzano annunci classificati e siti web di escort, social media e app di incontri, servizi di messaggistica e persino mercati darknet per reclutare, pubblicizzare, controllare e sfruttare le vittime. Analisi internazionali hanno ripetutamente riscontrato il reclutamento e la pubblicità tramite Internet nei casi di tratta; ad esempio, gli studi sui dati dei casi dell'UNODC e la mappatura dell'OSCE identificano i siti di escort, i siti web di massaggi/servizi sessuali e i social media come canali comuni. Negli Stati Uniti, la *National Human Trafficking Hotline* e *Polaris* hanno documentato centinaia di casi di reclutamento online e identificato migliaia di contatti collegati alla tratta facilitata dalla tecnologia. *Polaris* riferisce che dal 2015 la hotline ha segnalato **più di 950 potenziali vittime di tratta a scopo sessuale** reclutate online. Gli strumenti digitali modificano le modalità di applicazione della coercizione e del controllo (adescamento a distanza, annunci ingannevoli, monitoraggio tramite app di messaggistica e canali di pagamento) e

complicano anche le risposte perché le piattaforme attraversano i confini e operano in regimi giuridici diversi.

Piattaforme digitali utilizzate per lo sfruttamento sessuale

Poiché molte piattaforme mancano di moderazione, meccanismi di segnalazione e trasparenza nel modo in cui rispondono ai casi di sfruttamento, gli strumenti digitali e le piattaforme online sono ampiamente utilizzati nello sfruttamento sessuale in tutto il mondo. Ad esempio, OnlyFans ha presentato **230 segnalazioni** al *National Center for Missing & Exploited Children* (NCMEC), più **64 segnalazioni aggiuntive** presentate entro febbraio 2025, evidenziando le continue difficoltà nell'individuare i contenuti che coinvolgono le persone di minore età.

Arrivano inoltre reclami ricorrenti relativi a contenuti espliciti che coinvolgono persone che sono state pubblicate sulla piattaforma senza il loro consenso.

Nell'agosto 2025, il commissario britannico contro la schiavitù ha avviato un'indagine sui siti di escort/annunci (ad esempio *Vivastreet*), descritti come "siti web di sfruttamento della prostituzione". Uno studio scozzese del 2021 ha osservato come tali piattaforme abbiano potenziato il commercio del traffico sessuale.

Oltre alle piattaforme di escort e di contenuti per persone adulte, le/i trafficanti utilizzano massicciamente anche le piattaforme di social media mainstream come Tinder, Instagram e TikTok, nonché i mercati online e persino le piattaforme di giochi online come Roblox, Minecraft o Hago. Le piattaforme che combinano la popolarità tra le/i giovani con funzionalità sociali (come chat, voce, avatar e ricompense) sono diventate terreno fertile per gli abusi. La portata del *grooming*, la velocità con cui si sviluppa e il suo frequente collegamento a piattaforme esterne ai giochi stessi (come Discord o Snapchat) sottolineano l'urgente necessità di migliorare la progettazione della sicurezza, i sistemi di moderazione e la consapevolezza dei genitori e del personale educativo. Le piattaforme di gioco sono utilizzate in particolare per prendere di mira giovani e bambine/i. Le segnalazioni di sfruttamento su Roblox sono aumentate da **675 nel 2019 a oltre 24.000 nel 2024,** mettendo in luce la portata del problema.

- **Social media e app di messaggistica**

Le/i trafficanti utilizzano piattaforme mainstream come Facebook, Instagram, TikTok, LinkedIn, WhatsApp e Telegram per reclutare, adescare e controllare le vittime, spesso fingendosi amiche o amici, partner sentimentali o datrici/datori di lavoro. I social media consentono di individuare facilmente le persone vulnerabili e di utilizzare canali di comunicazione privati che nascondono lo sfruttamento. I profili Instagram, ad esempio, possono essere camuffati da annunci di escort e contenere dettagli di contatto nelle biografie o nelle storie. Alcune ONG in Francia e nel Regno Unito hanno documentato casi di trafficanti che creano false agenzie di modelle su Instagram per adescare giovani donne.

Su LinkedIn o Indeed, le/i trafficanti si fingono datrici/datori di lavoro o responsabili delle risorse umane e contattano direttamente persone giovani o disoccupate per offrire loro, ad esempio, "lavoro all'estero" o "guadagni elevati senza esperienza richiesta".

- **Piattaforme di gioco online**

Anche le piattaforme di gioco online vengono utilizzate in modo improprio per adescare, costringere o sfruttare sessualmente bambine/i e adolescenti. In genere, le adescatrici/gli adescatori conoscono le vittime durante il gioco e le costringono a condividere materiale esplicito o a incontrarsi di persona. È stato segnalato che alcune persone adulte attirano le bambine e i bambini utilizzando le valute dei giochi (come Robux di Roblox) per indirizzarle verso app come Discord o Snapchat e sfruttarle.

- **Siti web di incontri e escort**

Le app e i siti web progettati per gli incontri (ad esempio Tinder, Bumble) o i servizi sessuali commerciali/di escort sono spesso utilizzati per pubblicizzare vittime sotto coercizione. Gli annunci possono essere difficili da identificare perché mascherano lo sfruttamento come lavoro sessuale consensuale. Su Tinder, le/i trafficanti possono fingersi potenziali partner e instaurare un rapporto di fiducia prima di manipolare le vittime e sfruttarle sessualmente. In genere, utilizzano la funzione di abbinamento basata sulla posizione per identificare persone vulnerabili (persone migranti, rifugiate o in viaggio) nelle zone di confine o nei nuovi Paesi ospitanti, in modo da offrire loro "aiuto" o "lavori" che portano allo sfruttamento, come opportunità di lavoro come modelle o sugar baby.

- **Annunci e mercati online**

A volte, le/i trafficanti pubblicano annunci di lavoro ingannevoli (ad esempio, lavoro come modella, nel settore alberghiero o come ragazza alla pari) su mercati globali di annunci o equivalenti locali. Le vittime possono essere attirate in situazioni di sfruttamento con il pretesto di un lavoro legittimo. Per identificare e avvicinare le persone vulnerabili, le/i trafficanti sfruttano anche annunci falsi per camere, beni di seconda mano o "amicizia" come punti di ingresso. Le persone migranti in cerca di alloggi a prezzi accessibili su Facebook Marketplace, ad esempio, vengono prese di mira con "offerte" legate allo sfruttamento sessuale.

- **Piattaforme di live streaming e contenuti per persone adulte**

Le/i trafficanti sfruttano le vittime attraverso atti sessuali trasmessi in diretta streaming su siti di sesso tramite webcam o caricando contenuti ottenuti con la coercizione su piattaforme in abbonamento. Inoltre, costringono le vittime (tra cui bambine/i, persone migranti o adulte e vulnerabili) a esibirsi davanti alla telecamera attraverso minacce, violenza o schiavitù per debiti. Le vittime sono spesso rinchiuse in stanze, sorvegliate o private dei guadagni mentre le/i trafficanti controllano i loro account. In alcuni casi, le/i trafficanti costringono le vittime a incontrare i clienti offline dopo gli "spettacoli" online come

trampolino di lancio per la prostituzione di persona. Le piattaforme possono anche essere utilizzate per la *sextortion*. Il pubblico o le/i trafficanti registrano le vittime senza il loro consenso e utilizzano le riprese per ricattarle ("esibisciti di nuovo o questo video diventerà pubblico").

- **Mercati *darknet* e servizi crittografati**

I servizi nascosti sul *darknet* facilitano la pubblicità e la distribuzione di materiale di sfruttamento e sono difficili da monitorare per le forze dell'ordine.

Misure di protezione

La protezione delle persone richiede una strategia su più fronti: una moderazione rigorosa delle piattaforme e la segnalazione obbligatoria, un sistema di rilevamento potenziato dalla tecnologia per le forze dell'ordine, la regolamentazione delle piattaforme di servizi per persone adulte e risorse di empowerment per creator, giovani e gruppi vulnerabili.

Le piattaforme dovrebbero essere legalmente obbligate a segnalare alle autorità le attività sospette, richiedere controlli proattivi dell'identità, implementare un solido screening di immagini/video e verificare la gestione delle denunce di sfruttamento. I siti web di escort dovrebbero essere regolamentati per prevenire abusi e le forze dell'ordine dovrebbero utilizzare strumenti di rilevamento basati sull'intelligenza artificiale per identificare i modelli di traffico nelle inserzioni di escort.

Per proteggere le persone migranti è necessario aumentare la consapevolezza e l'informazione sui rischi delle truffe di reclutamento online e dello sfruttamento sessuale. In particolare, i centri comunitari, le ONG e i servizi locali dovrebbero insegnare alle persone migranti come verificare le offerte online, proteggere la loro privacy e utilizzare le piattaforme in modo sicuro. Tra le buone pratiche figurano i laboratori o l'educazione tra pari, che coinvolgono le/i leader delle comunità di persone migranti. I contenuti dovrebbero essere chiari e adattati culturalmente.

Soprattutto le persone giovani e le/i bambine/i devono essere consapevoli delle tattiche di adescamento online e dei "segnali di allarme" (ad esempio, la pressione a mantenere segrete le conversazioni, le richieste di immagini intime), mentre i genitori devono essere sensibilizzati sull'importanza dei controlli parentali, dei filtri per la privacy e delle funzioni di sicurezza delle piattaforme. Sono inoltre necessarie campagne di sensibilizzazione su questi temi nelle scuole, in altri ambienti educativi e nei media, nonché l'educazione delle operatrici e degli operatori sociali e del personale educativo.

Caso di studio: la migrazione in Guyana

La migrazione in Guyana è un fenomeno complesso e storicamente significativo che ha plasmato la demografia, l'economia e le connessioni globali del Paese.

L'intersezione tra migrazione, pressioni ambientali e sfruttamento digitale in Guyana rivela una serie di sfide complesse, soprattutto per le popolazioni vulnerabili delle regioni interne e costiere.

Rischi di sfruttamento digitale

Con l'aumento della migrazione, soprattutto tra le persone giovani e le donne, le piattaforme digitali diventano sia un'ancora di salvezza che una potenziale trappola:

- Truffe di reclutamento online: le persone migranti in cerca di lavoro all'estero o nelle aree urbane possono cadere vittime di offerte online fraudolente, che portano alla tratta di esseri umani o allo sfruttamento lavorativo.
- Vulnerabilità dei dati: la limitata alfabetizzazione digitale rende le persone migranti vulnerabili al furto di identità, al phishing e all'uso improprio delle informazioni personali.
- Sfruttamento di genere: le donne e le ragazze che emigrano per lavoro o per motivi di studio sono esposte a rischi maggiori di *sextortion*, cyberbullismo e molestie online.

Difficoltà e sfide in Guyana

- Divario digitale: le comunità dell'entroterra e quelle indigene spesso non dispongono di un accesso affidabile a Internet, il che le rende digitalmente invisibili e vulnerabili.
- Protezioni legali limitate**:** i quadri normativi della Guyana in materia di migrazione e sicurezza digitale sono ancora in evoluzione e presentano diverse lacune nella protezione delle persone sfollate a causa dei cambiamenti climatici e di quelle vulnerabili allo sfruttamento digitale.
- Fiducia e barriere culturali: gli studi dimostrano che la fiducia nei servizi di e-government è bassa e che i fattori culturali ostacolano l'adozione di misure di sicurezza digitali.
- Pressioni geopolitiche: le dispute territoriali e i cambiamenti nel mercato del lavoro aggiungono complessità alla governance della migrazione.

Soluzioni emergenti

- Hub ICT nelle regioni dell'entroterra: sono stati creati oltre 200 hub per migliorare l'accesso digitale, l'istruzione e i sistemi di allerta precoce per gli eventi climatici.
- Espansione dell'e-government: la Guyana sta investendo nella governance digitale per migliorare l'erogazione dei servizi e ridurre i rischi di sfruttamento.
- Coinvolgimento della diaspora: sono in fase di sviluppo programmi per sfruttare le competenze e le risorse delle cittadine e dei cittadini della Guyana all'estero, proteggendo al contempo coloro che emigrano.

La rapida espansione delle infrastrutture digitali in Guyana ha portato sia opportunità che rischi. Se da un lato gli strumenti digitali hanno dato più potere alle cittadine e ai cittadini e migliorato i servizi pubblici, dall'altro sono stati anche utilizzati come arma di sfruttamento.

Gli strumenti digitali più utilizzati per lo sfruttamento in Guyana

- Piattaforme di social media (Facebook, WhatsApp, Instagram): utilizzate per *phishing*, furti d'identità, *sextortion* e truffe di reclutamento. Le sfruttatrici e gli sfruttatori spesso si fingono datrici/datori di lavoro, partner sentimentali o agenti governativi per guadagnarsi la fiducia e accedere ai dati personali.
- E-mail di *phishing* e link dannosi: inviati tramite e-mail o app di messaggistica, questi link inducono gli utenti a rivelare le password o a scaricare malware. Le truffe più comuni includono falsi avvisi bancari, offerte di lavoro o comunicazioni governative.
- Botnet e malware: i criminali utilizzano dispositivi infetti per lanciare attacchi remoti o rubare dati. Queste reti possono essere utilizzate per furti di identità, frodi finanziarie o per diffondere contenuti illegali.
- Strumenti di ingegneria sociale: gli hacker utilizzano dati disponibili pubblicamente per manipolare le vittime tramite telefonate o messaggi diretti. Spesso si fingono agenti del servizio clienti o funzionari per estrarre informazioni sensibili.
- Spyware e PUP (programmi potenzialmente indesiderati): questi sono nascosti nei download e possono monitorare l'attività degli utenti, rubare dati o disabilitare le funzionalità di sicurezza.

Misure di protezione

- Politiche e legislazione in materia di sicurezza informatica**:** la Guyana ha implementato 43 politiche di sicurezza informatica in tutte le agenzie governative per salvaguardare l'infrastruttura digitale. Leggi come il *Data Protection Act* e il *Digital Identity Card Act* mirano a proteggere la privacy degli utenti e a garantire la sicurezza delle transazioni online.

- Formazione nazionale sulla sicurezza informatica: i funzionari pubblici vengono formati per individuare e rispondere alle minacce informatiche. Eventi come la Cybersecurity Fair riuniscono esperte ed esperti i per workshop e dimostrazioni dal vivo.

- Sistemi pubblici intelligenti: sistemi come *Safe Road Intelligent e-ticketing*, controllo automatizzato delle frontiere e cartelle cliniche elettroniche sono progettati con protocolli di sicurezza integrati.

- Piano generale per le TIC (2030): tabella di marcia strategica incentrata sull'efficienza digitale, la sicurezza e la resilienza in tutti i settori. Comprende sistemi di monitoraggio, quadri di valutazione e tecnologie avanzate per individuare e prevenire la criminalità informatica.

- Sensibilizzazione e istruzione della comunità: le ONG e le agenzie governative stanno lavorando per migliorare l'alfabetizzazione digitale, in particolare nelle comunità rurali e vulnerabili. Le campagne di sensibilizzazione sono rivolte alle persone giovani e alle donne, che sono colpite in modo sproporzionato dallo sfruttamento digitale.

4.3. Educare le comunità alla sicurezza digitale

Sebbene le piattaforme online stiano diventando sempre più una parte centrale della nostra vita, se utilizzate in modo irresponsabile possono anche comportare gravi rischi. Le nuove tecnologie dell'informazione e della comunicazione hanno rivoluzionato la distribuzione dei media, l'accesso alle informazioni e la comunicazione globale. Tuttavia, possono al contempo facilitare lo sfruttamento sessuale a livello locale, nazionale e internazionale (Hughes, 2002).

È essenziale che tutti gli stakeholder della comunità diano priorità alla sicurezza digitale. Ciò include l'educazione all'uso di risorse aggiornate per combattere la violenza online e fornire alle persone di minore età e a quelle giovani le conoscenze sui rischi digitali e sulle strategie di prevenzione. In ambito educativo, un personale docente competente e consapevole svolge un ruolo fondamentale nel rafforzare l'alfabetizzazione digitale (Tomczyk, 2019). Le/i

responsabili delle politiche devono inoltre riconoscere le bambine e i bambini come partecipanti attivi nel mondo digitale in grado di interagire in modo significativo con le informazioni (Patterson et al., 2022).

Nel complesso, l'obiettivo dell'alfabetizzazione digitale nel contesto della sicurezza su Internet è quello di promuovere un uso sicuro, creativo e consapevole dei media digitali (Kurniasih, 2023). Sebbene negli ultimi due decenni siano state avviate numerose iniziative per la sicurezza online volte a incoraggiare un comportamento online responsabile, c'è ancora margine di miglioramento nei metodi di attuazione (Quayle, 2020). A seconda del pubblico di destinazione, le risorse spaziano da quelle interattive a quelle esplicative, ciascuna delle quali offre preziose opportunità di coinvolgimento.

Le piattaforme digitali sono diventate fondamentali nella vita quotidiana delle persone giovani. Se, da un lato, offrono opportunità di apprendimento e comunicazione, dall'altro espongono le persone di minore età a rischi significativi, tra cui il **cyberbullismo, contenuti dannosi e sfruttamento sessuale** (Hughes, 2002).

La protezione delle bambine e dei bambini online richiede **l'impegno di tutta la comunità**. Le scuole, le famiglie e le autorità locali hanno tutte un ruolo nello **sviluppo dell'alfabetizzazione digitale e della consapevolezza**:

- Il **corpo docente** può fornire alle studentesse e agli studenti gli strumenti per riconoscere i rischi online e rispondere in modo efficace (Tomczyk, 2019).
- **I genitori e le/gli assistenti** hanno bisogno di una guida pratica per mediare l'uso degli schermi e discutere apertamente delle esperienze online.
- **Le/i responsabili delle politiche** devono garantire che le bambine e i bambini siano riconosciuti come **cittadini digitali attivi** e sostenuti da **solide misure di protezione** (Patterson et al., 2022).

Recenti studi illustrano la **portata e l'urgenza** di questa sfida.

Cifre chiave: rischi online per le persone giovani

Area di rischio	**Statistiche chiave**	**Fonti**
Cyberbullismo	Il 15% delle/degli adolescenti (≈1 su 6) ha subito cyberbullismo; il 29% nelle scuole superiori.	Santé Mentale, (2024); Jedha, (2025)

Esposizione a contenuti dannosi	**Età** media della prima esposizione alla pornografia: **10 anni**; il 70% delle persone tra gli 11 e i 18 anni ha visto contenuti inquietanti (violenza, pornografia, immagini di guerra).	Rapporto Élysée, (2023); Le Monde, (2024)
Tempo trascorso davanti allo schermo	Età 6-17 anni: **4h11/giorno**; adolescenti 13-19 anni: **7h+/giorno**; il 57% delle persone di età inferiore ai 20 anni riferisce effetti negativi.	GoStudent, (2025); INSEE, (2024)

Queste tendenze evidenziano la **crescente vulnerabilità digitale delle persone giovani**. Un'efficace educazione digitale non è solo una misura protettiva, ma **favorisce una partecipazione sana, consapevole e creativa** al mondo online (Kurniasih, 2023).

Per essere efficaci, le strategie comunitarie dovrebbero includere:

- **Intervento precoce nelle scuole**, a partire dall'istruzione primaria.
- **Coinvolgimento dei genitori e campagne di sensibilizzazione** per ridurre l'esposizione precoce a contenuti dannosi.
- **Quadri politici chiari** che colleghino la protezione delle persone di minore età, l'alfabetizzazione mediatica e la salute pubblica.

Combinando **istruzione, prevenzione e azioni politiche**, le comunità possono creare **ambienti digitali più sicuri e responsabilizzanti** per bambine/i e adolescenti.

Campagne educative sulla sicurezza digitale

Campagne video a livello europeo

- 63Campagna "Share with Care" di Deutsche Telekom per la condivisione di immagini e video di bambine/i online: https://youtu.be/F4WZ_k0vUDM.
- Campagna "Say No" di Europol contro il *catfishing* e l'estorsione sessuale: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime.

Esempi di risorse sulla sicurezza digitale delle persone migranti

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

Lingua: inglese. Una presentazione e note liberamente accessibili per il personale educativo, concesse in licenza Creative Commons, progettate per responsabilizzare le donne e le

ragazze migranti nell'Africa meridionale. Gli argomenti trattati includono molestie online, truffe, furto di identità e disinformazione.

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

- ***Tabliteracy – Digital Citizenship*** **(Irlanda)**

Lingua: inglese (progettato per studentesse e studenti con scarsa conoscenza della lingua inglese). Un dispositivo didattico basato su tablet che insegna la sicurezza online, la ricerca di lavoro, la ricerca di servizi, gli strumenti di comunicazione e l'integrazione locale in Irlanda. È basato su attività e adattato alle esigenze della vita reale.

GRECIA

Campagne sulla sicurezza digitale in Grecia per le persone giovani

Il Greek Safe Internet Centre [1] ha lanciato diverse campagne di grande impatto e fornito risorse pertinenti:

- **Concorsi per la Giornata per un Internet più sicuro[2]**: oltre ottocento (800) scuole hanno partecipato alla creazione di contenuti digitali su cyberbullismo, disinformazione e frodi online.
- **Concorso Capture the Flag (CTF)[3]**: ha introdotto le studentesse e gli studenti alla sicurezza informatica attraverso sfide pratiche di crittografia e informatica forense.
- **Pacchetti per il ritorno a scuola[4]**: includono risorse quali programmi didattici, quiz, video, poster e fiabe su misura per diverse fasce d'età.

Campagne sulla sicurezza digitale per persone adulte

Strategia nazionale per l'alfabetizzazione mediatica e le competenze digitali

Obiettivi centrali:

- Promuovere la sicurezza delle tecnologie digitali.
- Offrire opportunità di apprendimento correlate per le persone adulte.

Iniziativa europea per la sicurezza online

Si tratta di un progetto interattivo pensato sia per i genitori che per il corpo docente, con l'obiettivo di educare questi ultimi sui rischi associati ai media digitali. Fornisce risorse su:

- Cyberbullismo.

- Privacy su Internet.
- Questioni relative ai social media.

ESTONIA

In Estonia, diverse iniziative nazionali promuovono la sicurezza digitale e l'alfabetizzazione mediatica tra bambine/i, giovani, donne adulte e comunità di persone migranti. Queste iniziative forniscono alle scuole e alle organizzazioni comunitarie risorse pratiche, programmi didattici, workshop e campagne di sensibilizzazione.

- **Targalt Internetis (Navigare in modo intelligente sul web)**

Centro estone per un Internet più sicuro, coordinato da Harno e dall'Unione estone per il benessere delle/dei bambine/i. Fornisce:

  - Programmi didattici gratuiti, giochi interattivi e video su argomenti quali cyberbullismo, adescamento, privacy e impronte digitali.
  - Workshop in classe e visite scolastiche tenuti da esperte ed esperti qualificati.
  - Sessioni di formazione per insegnanti, operatrici/operatori giovanili e genitori.

- **Inspiratsioonikogumik**

Un toolkit pubblicato da Targalt Internetis che offre attività già pronte per il corpo docente. Include:

  - Esercizi in classe su cyberbullismo, etica online e impronte digitali.
  - Modelli adattabili per workshop con giovani e persone migranti.
  - Guide pratiche per affrontare i contenuti online dannosi.

- **Lasteabi (Linea di assistenza per l'infanzia 116111)**

Offre materiale didattico e consulenza riservata a bambine/i e famiglie. Le educatrici e gli educatori possono:

  - Utilizzare i moduli online per riconoscere e segnalare i pericoli online.
  - Invitare i consulenti a tenere conferenze nelle scuole o nei centri giovanili.

- Accedere a materiali di orientamento multilingue per le famiglie di persone migranti.

- **Campagne per la Giornata per un Internet più sicuro (coordinate da Harno e sostenute da Telia Estonia)**

Ogni febbraio, le scuole, gli asili, le biblioteche e i centri giovanili estoni partecipano ad attività di sensibilizzazione a livello nazionale coordinate da Targalt Internetis. Nel 2024, oltre 7.600 bambine/i hanno partecipato a 70 eventi. Le educatrici e gli educatori hanno ricevuto pacchetti di materiale tematico (video, test online, giochi) per organizzare sessioni e discussioni in classe. La conferenza principale, *Smartly on the Web: Digital Well-being and Mental Health (*"Usare Internet in modo intelligente: benessere digitale e salute mentale"*),* ha incluso workshop che hanno presentato nuovi strumenti come **ySKILLS, Triumfland Saga** e **Spoofy.** La campagna ha anche introdotto un **quiz sulla sicurezza informatica (*KüberNööpnõel*, CyberPin)** per le classi dal 1° al 6° anno e una **competizione di escape room digitale** per le classi dal 7° al 12° anno.

FRANCIA

Migliori pratiche e attività pratiche

- **Cybermalveillance.gouv.fr: *Cyber Guide Famille* e iniziative per giovani**
    - Offre strumenti didattici come fumetti, quiz, video in motion design e un quaderno di vacanze "As du Web" su misura per bambine/i dai 7 ai 14 anni.
    - Le attività possono essere adattate in classe: quiz interattivi, discussioni basate su scenari ed esercizi per diventare "supereroine" e "supereroi" digitali. Assurance Prévention+7Education Ministère+7cnil.fr+7CYBERMALVEILLANCE.GOUV.FR

- **CNIL: workshop e giochi sulla protezione dei dati**
    - Fornisce kit specifici per età (*Tous ensemble, prudence sur Internet !*) per bambine/i di età compresa tra 8 e 11 anni e ragazze/i di età compresa tra 11 e 15 anni.
    - Include giochi, video, attività stampabili e libretti "Incollables®" per insegnare la protezione dei dati personali attraverso sfide ludiche.
    - Il personale educativo può utilizzarli come moduli didattici o assegnare workshop ai genitori: cnil.fr+1CYBERMALVEILLANCE.GOUV.FR+1.

- ***Internet Sans Crainte*: giornata per un Internet più sicuro in Francia**
    - Workshop annuali per la Giornata per un Internet più sicuro con kit a tema (ad esempio, IA e cittadinanza digitale, *escape room* come *Vinz et Lou*).
    - Moduli pronti all'uso per il ciclo 2, 3 e le scuole superiori, progettati per essere utilizzati in classe o in sessioni guidate dai pari: CYBERMALVEILLANCE.GOUV.FR+3Better Internet for Kids+3Teachit+3.

- ***Promeneurs du Net* (PdN): mentorship digitale**
    - Operatrici e operatori giovanili professionisti si impegnano online per supportare le/i ragazze/i dai 12 ai 25 anni attraverso una presenza online strutturata.
    - Le attività comprendono sessioni di chat moderate, gruppi di discussione tra pari sui rischi digitali, simulazioni di giochi di ruolo e sessioni di domande e risposte nei centri giovanili o online (Wikipedia).

- **CLEMI: laboratori di alfabetizzazione mediatica e pensiero critico**
    - Attraverso la rete gestita dal Ministero, il CLEMI fornisce programmi didattici e schede informative per l'educazione all'alfabetizzazione mediatica, tra cui l'analisi dei social media, l'individuazione delle fake news e l'uso civico dei media.
    - Il corpo docente gestisce progetti come giornali studenteschi o esercizi di decodifica di foto/media per sviluppare competenze digitali critiche (Wikipedia).

- ***Académie de Créteil*: guida *Forming à la cybersécurité***
    - Un opuscolo di 13 pagine per le scuole che tratta: nozioni di base sulla sicurezza informatica, protezione dei dati, identificazione dei tentativi di phishing e abitudini sicure nell'uso dei dispositivi.
    - Progettato per lavori di gruppo o workshop nelle scuole medie e superiori: Better Internet for Kids+2dane.ac-creteil.fr+2Assurance Prévention+2cnil.fr.

- **Le 8 raccomandazioni della CNIL: laboratori co-progettati con bambine/i**

    - La CNIL ha sviluppato e co-creato laboratori con le/i bambine/i per spiegare concetti quali il consenso, i diritti alla privacy e l'autonomia sicura.
    - Formato suggerito: sessioni interattive in cui le/gli adolescenti contribuiscono alla progettazione di flussi UI o messaggi comprensibili (cnil.fr).

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

Una serie di materiali didattici (video, infografiche, diapositive) disponibili gratuitamente e scaricabili per insegnare la cittadinanza digitale, che coprono la privacy, i diritti online, la distinzione tra contenuti legali e illegali e l'alfabetizzazione mediatica. Ottimo per il personale che lavora con le persone migranti (Portale didattico).

- **ContreLaTraite.org: centro risorse**

Un ampio archivio di risorse online (in francese) con e-learning, guide, campagne e supporto per professioniste/i, in particolare sulla tratta di esseri umani in contesti che coinvolgono le persone migranti. Offre una vasta gamma di materiali (formazione, strumenti di prevenzione, informazioni sulle campagne) che possono essere adattati o utilizzati direttamente nei programmi incentrati sulle persone migranti: https://contrelatraite.org/centre-ressources.

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

Un ricco archivio che offre strumenti e guide per accompagnare digitalmente le persone vulnerabili, tra cui sicurezza informatica, mediazione digitale, sostegno ai genitori e giochi didattici multimediali: https://lesbases.anct.gouv.fr/ressources/ressources-pedagogiques.

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

Progettato per giovani dai 12 anni in su, questo marsupio virtuale contiene accessori (telefono, chiavi, taccuino, ecc.) che fungono da strumenti per imparare e riflettere su una serie di argomenti relativi alla vita emotiva e sessuale, all'uguaglianza di genere e alla violenza di genere e sessuale, compresa la prostituzione e lo sfruttamento sessuale: https://dansmabanane.mouvementdunid.org/.

- **Trousse pour les jeunes: sécurité en ligne (Canada)**

Destinato alle persone adolescenti (13-14 anni), questo kit di strumenti canadese spiega le forme di sfruttamento sessuale online come il *sexting*, la *sextortion,* il *grooming e* il *capping* (registrazione non consenziente di atti sessuali con lo scopo di minacciare la vittima) con diapositive, note e consigli per incoraggiare le vittime a parlare (Governo del Canada).

- **Malettes pédagogiques: CVM (Collectif contre la violence du marché sexuel)**

Queste risorse digitali forniscono materiali a genitori e professioniste/i per affrontare e prevenire la prostituzione minorile, e includono video, guide e risorse di sensibilizzazione (association-cvm.org Droit d'Enfance).

🧪 Esempi di attività da svolgere in classe

Fascia d'età	**Attività**	**Obiettivo**	**Formato**
7-11 anni	Creazione di fumetti: rappresentare messaggi sicuri e non sicuri	Comprendere la privacy e la condotta digitale	Lavoro di gruppo e presentazione
11-15 anni	Escape room "Usciamo dall'IA") (*Vinz et Lou*)	Riconoscere i rischi dell'IA e la cittadinanza digitale	Gioco di ruolo
Scuola media/liceo	Workshop sulle fake news con schede CLEMI	Sviluppare il pensiero critico e l'alfabetizzazione mediatica	Dibattito in classe e produzione digitale
Adolescenti online	Sessione live con *Promeneurs du Net*	Dialogo aperto su cyberbullismo, privacy e *sexting*	Chat moderata
Genitori e figlie/i	Quiz sulla protezione dei dati della CNIL per le famiglie	Stimolare la discussione a casa e a scuola	Opuscolo/workshop da portare a casa

Come utilizzare queste risorse in modo efficace

- Combinazione di formati didattici: è possibile combinare video, quiz interattivi, fumetti, discussioni di gruppo, attività fisiche e compiti digitali.
- Co-creazione di contenuti: le/i giovani progettano cartelloni sulla sicurezza, campagne mediatiche o flussi UX per le impostazioni sulla privacy, con la facilitazione del corpo docente.
- Coinvolgimento dei genitori: risorse da portare a casa o workshop congiunti (ad esempio, opuscoli CNIL o schede informative Cyber Guide).
- Mentorship tra pari: per condurre le sessioni è possibile coinvolgere le/i giovani "ambasciatrici" e "ambasciatori" digitali dei team PdN o Safer Internet Day.

- Apprendimento progressivo: iniziare con concetti semplici (ad esempio, nozioni di base sulla privacy nella scuola primaria) e passare ad argomenti più complessi, come la disinformazione e l'intelligenza artificiale, a livello secondario.

ITALIA

- Progetto **BEAWARE** (Francia, Italia, Grecia, Portogallo, Belgio, Cipro) - *Understanding, preventing, detecting and addressing Online Sexual Exploitation and Abuse (OSEA) attraverso un approccio olistico, multiforme e multisettoriale.*

  Risorse:

  - Il toolkit per operatrici e operatori è progettato per fornire approfondimenti teorici su argomenti relativi alla sicurezza online, ai rischi e ai pericoli sulle piattaforme online. Fornisce inoltre suggerimenti pratici su come affrontare episodi di abuso online e su come relazionarsi con le persone giovani che li segnalano.
  - L'app mobile per giovani affronta diversi argomenti attraverso sfide interattive. Può essere utilizzata anche in gruppo.
  - La piattaforma di apprendimento è uno spazio online che consente alle operatrici e agli operatori giovanili di acquisire una comprensione più ampia dell'alfabetizzazione digitale su argomenti rilevanti e di diventare più consapevoli di come affrontare tali questioni quando interagiscono con le persone giovani.

- Progetto **CESAGRAM** (Belgio, Grecia, Italia, Regno Unito, Lituania) - *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.*

  Risorse:

  - La biblioteca dispone di una moltitudine di fonti da cui attingere e informarsi.
  - Consulenza utile per i genitori sui materiali relativi agli abusi sessuali su persone di minore età per la sicurezza online.
  - Mappatura delle informazioni pratiche fornite da organizzazioni esperte sulla richiesta di supporto e maggiori conoscenze in materia.

CAMPAGNE:

Iniziative nazionali in Italia

Secondo l'Istituto Nazionale di Statistica, il 6,8% delle donne ha ricevuto proposte inappropriate o commenti osceni o maliziosi attraverso i social network nel corso della propria vita (Consiglio Regionale del Piemonte, 2022). La prevalenza delle molestie online è in aumento, in linea con il crescente utilizzo dei social network negli ultimi anni. Nel caso delle vittime di sesso femminile, il 44% delle molestie sui social media si è ripetuto più volte (ibidem). Tuttavia, nonostante il crescente allarme sul fenomeno, le iniziative sono ancora generiche e non sufficientemente adattate alla dimensione digitale e ai relativi rischi (Lavoce.info, 2025). In Italia, le donne possono contare su sistemi di supporto efficaci e molto rinomati anche per affrontare episodi di violenza online.

- **Numero verde 1522**

  Numero verde nazionale attivo 24 ore su 24 per assistenza e informazioni in caso di violenza o stalking. Il servizio è anonimo e riservato.

- **Telefono Rosa 06.37.51.82.82**

  È stato reso disponibile dall'Associazione Nazionale Volontarie del Telefono Rosa Onlus (www.telefonorosa.it). Attivo anch'esso 24 ore su 24, il servizio mira a fornire assistenza, sostegno e consulenza alle donne vittime di violenza o di qualsiasi forma di abuso, offrendo un ascolto attento e qualificato e un supporto nella comprensione dei loro diritti e delle possibili azioni da intraprendere per uscire dalla situazione di pericolo.

In Italia non sono state individuate campagne governative mirate. Tuttavia, alcune ONG si occupano effettivamente della prevenzione della violenza di genere online; di seguito è riportato un riepilogo di alcune delle più rilevanti.

- Il progetto CONVEY mirava a combattere la violenza sessuale e le molestie contro le donne promuovendo l'educazione tra pari tra persone giovani. Si concentrava sulla sensibilizzazione circa l'impatto degli stereotipi di genere e della sessualizzazione nei media digitali. Attraverso lo sviluppo di un gioco di simulazione educativo e di un programma pilota sulla parità di genere, l'educazione sessuale e l'alfabetizzazione mediatica, il progetto incoraggiava il cambiamento comportamentale. CONVEY ha anche sostenuto il corpo docente con un programma di formazione per aiutare le scuole a promuovere il rispetto dei diritti delle donne e a prevenire gli stereotipi di genere nella società digitale odierna, sviluppando al contempo raccomandazioni politiche.

- Il progetto CHASE mirava ad affrontare il crescente problema dell'incitamento all'odio online basato sul genere, sviluppando e implementando un meccanismo di risposta globale a Cipro, in Italia, Grecia e Francia. Si è concentrato sul miglioramento delle strategie di individuazione e reazione all'interno delle piattaforme mediatiche online. Riconoscendo la mancanza di dati disaggregati per genere e la limitata ricerca sulla violenza informatica, CHASE ha cercato di colmare queste lacune e sostenere la creazione di spazi digitali più sicuri. Il progetto contribuisce a politiche UE più efficaci e coordinate contro la violenza di genere online e l'incitamento all'odio.

- EmpowerTech è un progetto di formazione digitale promosso da D.i.Re e dall'Università della Calabria, pensato per le attiviste e gli attivisti che lavorano nei centri antiviolenza. Il programma si svolge online e si concentra su tre obiettivi principali: migliorare la sicurezza nella gestione dei dati sensibili e nell'uso consapevole degli strumenti digitali; aumentare l'efficienza del lavoro attraverso l'uso di strumenti digitali gratuiti e open source; promuovere il benessere personale e collettivo attraverso tecniche volte a ridurre lo stress e migliorare la collaborazione. L'iniziativa mira a rafforzare le competenze digitali delle attiviste e degli attivisti, favorendo un ambiente di lavoro più sicuro, più efficace e più solidale.

- **"PARLIAMONE!"** - Un progetto lanciato in un liceo di Palermo, che include un **manuale digitale** per le operatrici e gli operatori giovanili per affrontare il bullismo e il cyberbullismo nei confronti delle persone LGBTQIA+.

- **Progetti scolastici "Differenza Donna"** - Una serie di iniziative (2008-2023) volte a prevenire comportamenti aggressivi e a promuovere l'educazione alla parità di genere nelle scuole primarie e secondarie di Roma, tra cui *Scuole in Rete contro la Violenza*, *Pari e Dispari* e *Facciamo la differenza*.

- **Progetto ADA – Aumentare le competenze digitali nei centri antiviolenza,** finanziato dal *Fondo per la Repubblica Digitale* (2025-2026) - Fornisce al personale dei centri antiviolenza competenze digitali, concentrandosi sulla violenza di genere online, l'attivismo e la comunicazione digitale.

- **Safer Internet Day - Generazioni Connesse:** giornata internazionale di sensibilizzazione (seconda settimana di febbraio) dedicata alla sicurezza online, coordinata in Italia da **Generazioni Connesse** in collaborazione con il Ministero dell'Istruzione, la Polizia Postale, Save the Children e altri partner.

- **Una vita da social** - Campagna itinerante della **Polizia di Stato italiana**, parte del progetto Generazioni Connesse, che mira a sensibilizzare milioni di studentesse,

studenti, insegnanti e famiglie sui rischi di Internet attraverso incontri nelle scuole e nelle piazze pubbliche.

- **Noi cittadini digitali** - Iniziativa di **Trend Micro** e **JA Italia** volta a sviluppare una cultura consapevole dell'uso di Internet. Offre laboratori per studentesse e studenti delle scuole medie e rilascia una "patente di cittadinanza digitale" in occasione della Giornata per un Internet più sicuro.
- ***Cybercity Chronicles* – Campagna *Be Aware Be Digital* -** Un videogioco educativo ("edutainment") creato dal **DIS** (Dipartimento Informazioni e Sicurezza) in collaborazione con il Ministero dell'Istruzione per sensibilizzare le studentesse e gli studenti delle scuole medie sui rischi online.

4.4. L'impatto del settore privato

Lungi dall'essere piattaforme passive, le aziende tecnologiche di oggi sono attivi promotori della sicurezza digitale. I social network, le app di messaggistica e altri servizi online si sono evoluti fino a diventare i primi difensori contro i danni informatici basati sul genere. Il loro ruolo di *gatekeeper* non è solo normativo, ma a volte anche visionario. Perfezionando gli algoritmi, migliorando i protocolli di moderazione e salvaguardando i dati degli utenti, queste aziende non solo mitigano gli abusi, ma spesso li anticipano prima che si aggravino. Il settore privato è in grado di rispondere più rapidamente rispetto alla legislazione e di adattarsi alle minacce emergenti con precisione e su larga scala.

Progettare con empatia e lungimiranza

La progettazione etica non è solo un semplice requisito, ma anche un vantaggio competitivo. Le aziende lungimiranti stanno integrando principi sensibili alle questioni di genere direttamente nei loro cicli di sviluppo dei prodotti. Ciò significa creare funzionalità che scoraggino lo stalking, le molestie e la condivisione non consensuale dei dati, promuovendo al contempo l'autonomia e la sicurezza degli utenti. A differenza dei mandati burocratici, queste innovazioni sono guidate dalla reattività del mercato e dal desiderio genuino di servire una base di utenti diversificata. La capacità del settore privato di iterare rapidamente garantisce che le considerazioni etiche siano funzionali, testate dagli utenti e, quindi, efficaci.

La responsabilità come imperativo aziendale

La trasparenza è un imperativo fondamentale dell'etica aziendale. Le aziende tecnologiche pubblicano sempre più spesso rapporti dettagliati sui casi di abuso, sui risultati della moderazione e sulle metriche di sicurezza degli utenti, non perché sono obbligate a farlo, ma perché la fiducia è la loro valuta. Gli audit etici e le revisioni da parte di terzi stanno diventando una pratica standard che rafforza l'impegno del settore nei confronti dei diritti

fondamentali. In molti casi, le aziende stanno fissando standard più elevati di quelli richiesti dalle autorità di regolamentazione, dimostrando che la responsabilità può essere un obiettivo autonomo piuttosto che un obbligo reattivo.

Collaborazione strategica con attori della società civile e organizzazioni di base

Le aziende private non lavorano in modo isolato, ma stringono potenti alleanze con ONG e gruppi di sostegno. Queste partnership hanno portato allo sviluppo di strumenti di segnalazione più intelligenti, sistemi di supporto più empatici per le vittime e campagne di sensibilizzazione che risuonano a livello globale. Il mondo aziendale apporta dimensioni, infrastrutture e competenze tecniche; la società civile apporta esperienze vissute e conoscenze di base. Insieme, stanno colmando le lacune di capacità e costruendo quadri completamente nuovi per la sicurezza digitale.

Inoltre, i programmi di formazione condotti dalle ONG aiutano le/gli sviluppatori e le/i moderatori a interiorizzare la sensibilità di genere; tuttavia, sono le aziende stesse a investire in questi sforzi, in quanto riconoscono che le piattaforme inclusive sono più sostenibili e più redditizie. Anche nella difesa delle politiche, il settore privato non è più un partecipante riluttante, ma un alleato proattivo, che presta la sua voce e le sue risorse per plasmare una legislazione che rifletta le dinamiche reali della tecnologia digitale.

L'innovazione come scudo contro lo sfruttamento

Il contributo più potente del settore privato alla sicurezza digitale risiede nella sua capacità di innovazione. Gli strumenti di moderazione basati sull'intelligenza artificiale ora rilevano in tempo reale il linguaggio offensivo, lo sfruttamento basato sulle immagini e le molestie coordinate, un risultato che gli esseri umani non potrebbero ottenere su larga scala. Queste tecnologie sono anche predittive, imparano dai modelli per prevenire i danni prima che si verifichino (e non si limitano a reagire agli atti perpetrati).

La progettazione incentrata sulla privacy è un altro segno distintivo dell'ingegnosità aziendale. La messaggistica diretta con crittografia end-to-end, la segnalazione anonima e le impostazioni di visibilità personalizzabili consentono agli utenti di riprendere il controllo della propria vita digitale. Non si tratta di caratteristiche marginali, ma fondamentali, plasmate dalla domanda degli utenti e dalla lungimiranza etica. Inoltre, quando si tratta di protezione dei dati, le aziende sono leader grazie a una crittografia robusta, un accesso minimo da parte di terzi e misure di sicurezza interne, tutte caratteristiche che stanno diventando norme del settore, soprattutto quando si tratta di dati sensibili come la salute riproduttiva o il tracciamento della posizione.

CONCLUSIONI

5. Conclusioni

Nella lotta costante per proteggere le donne dallo sfruttamento online, le associazioni e i gruppi di difesa dei diritti si trovano ad affrontare un sistema che spesso è strutturalmente impreparato alle realtà e all'evoluzione della criminalità digitale. Le/i trafficanti operano con un certo grado di impunità oltre i confini nazionali, sfruttando l'assenza di una legislazione internazionale coerente e l'inerzia della cooperazione giudiziaria tra i Paesi. Mentre Internet non conosce confini, i sistemi di giustizia penale rimangono fondamentalmente nazionali e quindi lenti nella comunicazione, riluttanti a collaborare e talvolta paralizzati da definizioni giuridiche incompatibili di tratta, consenso e abuso digitale.

Per le donne che ne sono vittime, le conseguenze sono devastanti. Le sopravvissute sono costrette ad attendere a lungo che i tribunali determinino la giurisdizione, che le prove siano ammesse e che le autorità straniere rispondano. Le associazioni che lavorano per loro conto devono districarsi in una complessa rete di burocrazia, spesso affidandosi a reti informali e relazioni personali per portare avanti i casi. La mancanza di urgenza nella cooperazione transfrontaliera blocca i processi.

A questa complessità si aggiunge il mondo opaco delle criptovalute. Le/i trafficanti utilizzano sempre più spesso Bitcoin e altre valute digitali per trasferire denaro in modo anonimo, aggirando così i sistemi finanziari tradizionali ed eludendo i controlli. Sebbene la *blockchain* offra una tracciabilità teorica, nella pratica gli strumenti necessari per seguire queste tracce sono costosi, altamente tecnici e spesso fuori dalla portata delle forze dell'ordine. Le *privacy coin*, i *mixer* e gli scambi decentralizzati rendono ancora più oscure le transazioni finanziarie, consentendo alle persone responsabili di riciclare i profitti con un rischio minimo.

La sicurezza delle donne online non può essere messa in secondo piano: deve essere un pilastro centrale della governance digitale. Ciò significa costruire quadri giuridici internazionali che diano priorità alle popolazioni vulnerabili e ai diritti umani, investire nella formazione giudiziaria transfrontaliera, nelle banche dati condivise e nei protocolli di risposta rapida, nonché regolamentare i mercati delle criptovalute con la stessa vigilanza applicata alla finanza tradizionale; perché, come il denaro si muove nell'ombra, lo stesso vale per lo sfruttamento delle donne.

Bisogna ricordare che lo sfruttamento sessuale online non avviene nel vuoto, ma è profondamente radicato e sostenuto da strutture che traggono profitto dall'attenzione, dal

coinvolgimento e dal controllo. Le piattaforme dei social media e i servizi digitali sono progettati per dare priorità al profitto rispetto alla sicurezza, spesso amplificando contenuti sensazionalistici, violenti o sessualizzati per massimizzare il coinvolgimento degli utenti. Le industrie dello sfruttamento, dalla pornografia alla raccolta di dati, capitalizzano sulla mercificazione dei corpi delle donne, delle loro vite private e della loro vulnerabilità emotiva. In questo sistema, l'abuso di genere non è un difetto, ma una caratteristica: un sottoprodotto redditizio di un'economia digitale che valorizza la viralità rispetto alla responsabilità e l'esposizione rispetto al consenso.

Fino a quando tutti questi sistemi non si evolveranno, le associazioni continueranno a combattere battaglie in salita con strumenti limitati e determinazione illimitata. Il loro lavoro non riguarda solo la giustizia, ma anche il ripristino della dignità delle donne che sono state vittime di abusi su Internet, uno spazio altrimenti progettato per la libertà e la connessione.

BIBLIOGRAFIA

6. Bibliografia

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/anonymity

Camarda, 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

MADRES VICTIMAS DE TRATA
desaparecidas para ser prostituidas

KEMEA

élan interculturel

D'AILLEURS & D'ANTILLES

NOGAP
WHAT'S NORMAL?

cesie
the world is only one creature

beecom

femLENS

Cofinanziato dall'Unione europea

Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione Europea o dell'agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili

visit the Memory Library

on YouTube @WeLensProject