UNIVERSITÀ DEL SALENTO


# "DIVARI E DISCRIMINAZIONI DI GENERE NELLO SPAZIO DIGITALE EUROPEO. QUALI CONSEGUENZE? FOCUS SUL SEXIST HATE SPEECH ONLINE"

**SEMINARIO ORGANIZZATO DAL**
**LABORATORIO CRID SU DISCRIMINAZIONI E VULNERABILITÀ**
**UNIMORE**

~~

*MODENA – 15 novembre 2023*

*****

*Prof.ssa Claudia MORINI*

**********

**«[…] while the *gender digital divide* prevents vast portions of women and girls from enjoying these potential benefits – for those who are online and do have access, a growing body of evidence sheds light on the ways in which *the digital revolution has exacerbated existing, and even created new, forms of gendered inequalities and oppression*»**

(O'Donnell, A., and C. Sweetman, *Introduction: Gender, development and ICTs*, Gender & Development, 2018, 26 (2))

## Quali sono le sfide specifiche che le donne affrontano nel contesto digitale? → *Digital divide*; pregiudizi e discriminazioni; cyberviolenza; *sexist hate speech.*

Le **tecnologie e le soluzioni digitali** possono accelerare i progressi verso la parità di genere e l'emancipazione femminile in settori quali l'istruzione, l'occupazione e l'imprenditorialità, come pure verso la prevenzione e la lotta alla violenza di genere. Possono aiutare le donne a far fronte alle emergenze, come dimostrato dalla pandemia di COVID-19, attenuando le conseguenze socio-economiche e favorendo la resilienza. I servizi elettronici, come la finanza digitale, possono creare opportunità per l'emancipazione economica delle donne, migliorando il loro accesso ai servizi finanziari e aumentandone l'utilizzo da parte loro.

Il **divario digitale**, ovvero il divario tra chi ha accesso alle tecnologie digitali e alla connettività e chi non ce l'ha, influisce sulla capacità delle persone di partecipare all'era digitale e di coglierne le opportunità. Esso varia enormemente a seconda delle regioni geografiche e tra donne e uomini. Le donne che vivono in aree rurali o remote subiscono una triplice discriminazione (digitale, di genere e rurale) e affrontano enormi barriere all'accesso e all'uso delle tecnologie digitali per ragioni legate al costo di tali tecnologie, alla scarsa alfabetizzazione digitale e alle norme sociali.

Inoltre **la digitalizzazione comporta anche nuovi rischi e nuove sfide per la parità di genere**, ad esempio in termini di possibili pregiudizi di genere trasmessi dall'intelligenza artificiale o di un aumento della violenza di genere.

# I DIRITTI UMANI DELLE DONNE SONO UN BAGAGLIO CULTURALE RECENTE PER L'UMANITÀ

- Dalla fine della seconda guerra mondiale ad oggi lo sviluppo dei diritti umani e dei diritti delle donne ha portato consapevolezza sui diritti e la violenza
- La CEDAW-Convenzione per l'eliminazione di tutte le discriminazioni contro le donne del **1979** aggiunge nel **1992** la raccomandazione n. 19 sulla violenza sulle donne e nel **2017** la raccomandazione n. 35
- Conferenza ONU di Vienna 1993: i diritti umani sono diritti delle donne.. Istituita la figura della *Special rapporteur sulla violenza sulle donne, le sue cause e conseguenze*
- **1995**: Conferenza mondiale delle donne a Pechino: tra i 12 punti di criticità per raggiungere la parità c'è la violenza sulle donne
- **1999:** istituzione della Corte penale internazionale e viene riconosciuto lo stupro di guerra crimine contro l'umanità

**Prima del 1993 a livello internazionale la 'violenza di genere' non aveva nome!**

***Dichiarazione dell'Assemblea generale della Nazioni Unite sull'eliminazione della violenza contro le donne (adottata con Risoluzione 48/104 il 20 dicembre 1993)***

**Articolo 1.** - Ai fini della presente Dichiarazione l'espressione "violenza contro le donne" significa ogni atto di violenza fondata sul genere che abbia come risultato, o che possa probabilmente avere come risultato, un danno o una sofferenza fisica, sessuale o psicologica per le donne, incluse le minacce di tali atti, la coercizione o la privazione arbitraria della libertà, che avvenga nella vita pubblica o privata.

# LA VIOLENZA DI GENERE È UN PROBLEMA INNANZITUTTO CULTURALE….

- «States should condemn violence against women and should not invoke any custom, tradition or religious consideration to avoid their obligations with respect to its elimination. States should pursue by all appropriate means and without delay a policy of eliminating violence against women and, to this end, should: Adopt all appropriate measures, especially in the field of education, to modify the social and cultural patterns of conduct of men and women and to eliminate prejudices, customary practices and all other practices based on the idea of the **inferiority or superiority** of either of the sexes and on stereotyped roles for men and women».

***1993 Declaration on the Elimination of Violence against Women*, Articolo 4**

# STRUMENTI REGIONALI INTERNAZIONALI PER CONTRASTARE LA VIOLENZA SULLE DONNE

Dagli anni ‘90 in poi nascono Convenzioni regionali per contrastare la violenza contro le donne:

- **1994-1995 - Convenzione di Bélem do Pará Inter-Americana:** Convenzione per la prevenzione, la repressione, e l'eliminazione della violenza contro le donne
- **2005 - Protocollo di Maputo della Carta africana** dei diritti umani e dei popoli: sui diritti delle donne in Africa
- **2011- Convenzione del Consiglio d’Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica**, meglio conosciuta come Convenzione di Istanbul perché finalizzata e firmata in quella città. La Convenzione è entrata in vigore nel 2014, dopo aver raggiunto 10 ratifiche da parte dei Paesi membri.

# *OUTLINE* DEL SEMINARIO

- 1. Introduzione: il *cyberspace* come 'luogo' del diritto e dei diritti
- 2. Discriminazioni e violenza di genere: la dimensione *online* e c.d. '*technology-facilitated*'
- 3. L'applicazione del quadro giuridico internazionale in materia di diritti umani alla violenza di genere online
- 4. Il contesto regionale europeo
- 5. *Segue*. L'azione dell'Unione europea
- 6. Focus sull'*hate speech online* sessista contro le giornaliste
- 7. Riflessioni conclusive

# INTRODUZIONE

- Nelle società contemporanee le **tecnologie digitali** «can play an important role in empowering women and girls to exercise all human rights, including the right to freedom of opinion and expression, and in their full, equal and effective participation in political, economic, cultural and social life» (**HRC Res. 17/7/2018**). L'**emancipazione femminile**, dunque, si rafforza anche grazie alla promozione dell'accesso alle nuove tecnologie per tutte le donne, strumenti che ne favoriscono la partecipazione alla vita pubblica e possono costituire un importante ausilio anche nelle loro vite professionali.
- Invero, in un mondo sempre più digitalizzato e connesso, una delle più preoccupanti dinamiche riguarda però l'esasperarsi di episodi di violenza contro le donne "committed, assisted, aggravated or amplified by the use ICTs or other digital tools" (Harris, B. and L. Vitis. 2020. "Digital intrusions: Technology, spatiality and violence against women." Journal of Gender-Based Violence 4 (3), pp. 325–341).
- In questo contesto in chiaroscuro, lo spazio digitale rappresenta senz'altro un 'luogo' in cui poter esercitare i propri diritti, tra cui uno riconosciuto quale fondamentale dalla comunità internazionale, un vero e proprio 'elemento essenziale' delle nostre democrazie, ovvero la libertà di espressione: non è possibile, infatti, parlare di democrazia se manca o se è fortemente limitato un effettivo flusso di opinioni e un libero e aperto confronto tra esse.

- Al contempo, il *cyberspace* è purtroppo anche uno spazio in cui possono essere commesse violazioni di diritti/reati : molestie informatiche, *stalking* informatico, violazioni della *privacy*, registrazione e condivisione di immagini di violenza sessuale.

- Il cyberspace è un 'luogo' caratterizzano da specificità che rendono la questione della persecuzione dei presunti colpevoli più complessa a differenza di quanto avviene quando le violenze si consumano in un luogo fisico: a differenza della violenza fisica – che implica la presenza in un stesso luogo di tutti i soggetti coinvolti – quella online o resa possibile dalle tecnologie, può aversi anche a grande distanza e, quindi, la vittima può subire attacchi anche quando fisicamente non si trova in prossimità del suo aguzzino. In quei casi, purtroppo, neppure la propria abitazione o il luogo di lavoro possono dunque essere 'spazi sicuri'.

- Questa circostanza può causare maggiori difficoltà e ritardi nelle attività investigative e, aspetto molto rilevante, può comportare una non corretta e adeguata valutazione del rischio (c.d. risk assesment) cui è esposta la vittima, poiché non si può sapere se e quando la violenza 'a distanza' potrebbe poi tramutarsi anche in violenza fisica.

- Se in teoria sia le donne che gli uomini possono essere vittime di violenza informatica, tuttavia, è dimostrato che le donne e le ragazze sono altamente e maggiormente esposte ad essa. Non solo hanno maggiori probabilità di essere prese di mira dalla violenza informatica, ma possono subire gravi conseguenze, con conseguenti danni fisici, danni e sofferenze sessuali, psicologiche o economiche. La violenza informatica contro donne e ragazze (CVAWG) viene spesso liquidata come un fenomeno insignificante e virtuale. Tuttavia, essa è una violenza di genere che viene perpetrata attraverso le nuove tecnologie, ma è profondamente radicata nella disuguaglianza tra donne e uomini che ancora persiste nelle nostre società.

- Esistono molte forme diverse di CVAWG. Molte potrebbero essere viste come estensioni *online* di pratiche perpetrate *offline* (es. le molestie informatiche o il *cyber stalking*). Tuttavia, nel cyberspazio si perpetrano forme diverse e uniche di violenza di genere (es. abuso non consensuale dell'immagine intima o *doxing*) e possono amplificare la portata del danno rispetto alla violenza perpetrata nel mondo fisico.

- Queste pratiche si inseriscono nel *continuum* della violenza contro donne e ragazze e rappresentano un'ennesima forma di abuso e di 'silenziamento' incorporata nelle 'strutture di potere' di genere già esistenti. Gli atti violenti che avvengono attraverso la tecnologia sono parte integrante della stessa violenza che le donne e le ragazze sperimentano nel mondo fisico, per ragioni legate al loro genere.

## QUALI SONO I ‘MEZZI’ A DISPOSIZIONE DEGLI AUTORI DI TALI CONDOTTE?

Sono diversi i ‘mezzi’ attraverso i quali le diverse pratiche sulle quali ci soffermeremo a breve vengono perpetrate: si tratta di una vasta gamma di strumenti tecnologici che, purtroppo, pur avendo facilitato il nostro vivere quotidiano, sempre più spesso vengono usati impropriamente (c.d *misuse*) per perseguitare, molestare e controllare le vittime. Ecco, allora, che smartphone, computer, fotocamere e altri apparecchi di registrazione possono diventare armi affilate.

Inoltre, ampliando la nozione di ‘violenza’ a quella c.d. “facilitata dalla tecnologia”, potrebbero poi essere inclusi anche navigatori GPS o satellitari, orologi intelligenti, fitness trackers e dispositivi domestici smart, nonché tecnologie digitali dedicate al ‘controllo’ come *spyware* e *stalkerware*.

# QUALI SONO LE VITTIME ‘PRIVILEGIATE’?

Molto spesso la CVAWG è una forma intersezionale di violenza con diversi modelli e livelli di vulnerabilità e rischio per gruppi specifici di donne e ragazze.

Ad esempio, in un’indagine della FRA del 2014 condotta negli allora 28 Stati membri dell'Unione europea (UE), il 34% delle intervistate con disabilità avevano sperimentato violenza fisica, sessuale o psicologica e minacce di violenza (anche *online*), a confronto con il 19% delle donne che non avevano disabilità.

Particolarmente esposte a queste forme di violenza sono poi le donne lesbiche, bisessuali e transgender, così come le donne provenienti da gruppi di minoranze razziali e diverse comunità religiose.

In particolare, in relazione ai migranti, quando le seconde generazioni e determinate etnie o minoranze religiose sono oggetto di queste forme di violenza, esse sviluppano una minore fiducia nelle istituzioni e, in definitiva, ciò provoca seri danni all’integrazione sociale.

Ancora, come è noto, le donne sono ancora **sottorappresentate nei ruoli di *leadership* in tutto il mondo**; c'è, invero, un bisogno enorme di una maggiore diversità di genere in politica, nel giornalismo e in altre posizioni apicali; tuttavia, questa esigenza è soffocata quando le donne che sono riuscite a diventare 'leader' in ambiti importanti iniziano a subire molestie *online*.

Solitamente, i temi che scatenano maggiormente gli *haters* contro queste donne sono fortemente politicizzati, come il razzismo, il femminismo e la tutela dei diritti umani. Le vittime, purtroppo, in seguito a questi feroci attacchi, vedono fortemente messa alla prova la capacità di proseguire nel loro percorso di emancipazione e sviluppo personale. Oltre a questo danno *ad personam*, gli attacchi *online* di stampo sessista contro queste donne possono poi provocare un effetto sistemico di 'auto-esclusione' delle donne dalla ricerca di conseguire posizioni rilevanti e di prestigio in settori strategici delle democrazie contemporanee, per il timore di poter a loro volta essere vittime di tali attacchi.

Quale ‘nuova forma di violenza di genere’, **la cyberviolenza e quella facilitata dalla tecnologia**, presentano delle caratteristiche peculiari come ad esempio:

- la possibilità che si incorra nel c.d. *cross-jurisdictional abuse* (ovvero l’abuso delle esistenti differenze tra gli ordinamenti quanto a regolamentazione del fenomeno);
- la possibilità per i colpevoli di rimanere anonimi e di poter continuare a molestare la vittima ogni volta che essa utilizzi le tecnologie;
- la difficoltà di rimuovere dei contenuti digitali che, per loro natura, possono essere perenni;
- la facilità con la quale i contenuti possono essere copiati, salvati e diffusi;
- l’ampiezza di coloro che ‘assistono’ agli abusi e, in alcune ipotesi, la possibilità che più soggetti si uniscano al fine di perpetrarli

# LA DISCRIMINAZIONE E LA VIOLENZA DI GENERE: LA DIMENSIONE *ONLINE* E C.D. 'TECHNOLOGY - FACILITATED'

- In un **Report** del **18 giugno 2018**, lo *UN Special Rapporteur on violence against women* (A/HRC/38/47) fornì una definizione di 'violenza online e ICT-facilitated': "The definition of online violence against women […] extends to any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately" .
- Questa definizione è sufficientemente ampia da: a) enfatizzare la continuità della violenza di genere contro le donne sia *online* che *offline*; b) permettere di considerarla come un concetto quadro al quale si riferiscono diverse forme di GBVAW *online*. In riferimento alla violenza online si può anche ricorrere a termini assimilabili quali "violenza digitale" o "violenza informatica".

Di recente, nel ***General Comment N. 25 (2021) sui diritti dei bambini in relazione all'ambiente digitale***, il Comitato dei diritti dell'infanzia delle Nazioni Unite ha utilizzato anche l'espressione "violenza nell'ambiente digitale".

Nella ***Strategia sui diritti delle vittime 2020-2025***, la Commissione europea ha fatto ricadere nella fattispecie di **'criminalità informatica o *online*'** "qualsiasi tipologia di reato commesso in rete o mediante l'utilizzo di strumenti informatici o telematici", che "può includere reati gravi contro le persone, come i reati sessuali *online* (compresi quelli contro bambini), furto d'identità, crimini d'odio *online* e crimini contro il patrimonio (come frode e contraffazione di mezzi di pagamento diversi dai contanti)'.

Nonostante le definizioni che utilizzano il termine ‘online’ siano quelle maggiormente diffuse, occorre ricordare che *stricto iure* ‘online’ significa “connesso a una rete internet”. Invece, termini come ‘informatica’ o ‘cyber’ permettono di **ampliare il novero delle condotte violente perseguibili**.

Anche l’utilizzo del termine ‘tecnologie dell’informazione e della comunicazione (*ICTs*)’ si presenta particolarmente appropriato, in quanto si tratta del termine più ampio e atto a ricomprendere sia l’informatica che le tecnologie delle telecomunicazioni, con particolare attenzione al loro utilizzo combinato nell’elaborazione delle informazioni e nella trasmissione delle stesse.
In questo caso, emerge come il collegamento a una rete *internet* non sia strettamente necessario.

Tra i tipi di comportamento che costituiscono violenza facilitata dalle *ICTs*, il Relatore Speciale delle Nazioni Unite sulla violenza contro le donne, nel rapporto 2018 sopra menzionato, ha evidenziato innanzitutto le seguenti forme di violenza commesse *online*: alcune emergenti come il ***doxing***, la ***sextortion*** e il ***trolling***; altre, invece, sono forme di violenza che possono essere commesse anche *offline* ma che quando vengono commesse *online* implicano l'utilizzo del prefisso "online", come ***mobbing online***, ***stalking online*** e **molestie *online***.

Infine, viene anche menzionata la **distribuzione non consensuale di contenuti intimi**.

In linea con gli studi attuali, la ***cyber* violenza nel contesto della violenza di genere** è intesa come molestia *online*, incitamento *online* all'odio basato sul genere anche attraverso lo *stalking online*, le minacce *online*, la pubblicazione di informazioni o contenuti avente natura grafica intima senza consenso, l'accesso illegale a comunicazioni intercettate e ai dati privati e ogni altra forma di uso abusivo dell'informatica e delle comunicazioni da parte dell'interessato quali uso di computer, *smartphone* o altri dispositivi simili, che utilizzano le telecomunicazioni in grado di connettersi a *Internet* e di inviare *e-mail* o utilizzano piattaforme *social*, con l'obiettivo di sbugiardare, umiliare, spaventare, minacciare o mettere a tacere la vittima.

Volendo ampliare l'indagine anche alle **forme di violenza 'technology-facilitated'**, è opportuno dare conto di alcune 'definizioni' elaborate in diversi contesti, che hanno poi ispirato il lavoro di una Commissione di esperti istituita da *UN Women*.

**TFVAWG**:

1) "includes a range of different forms of violence perpetrated by ICT means on the grounds of gender or a combination of gender and other factors (e.g. race, age, disability, sexuality, profession or personal beliefs). Cyber violence can start online and continue offline, or start offline and continue online, and it can be perpetrated by a person known or unknown to the victim" - **European Institute for Gender Equality (EIGE)**;

2) “an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, against a person on the basis of their gender” - **United Nations Population Fund (UNFPA)**;

3) “action by one or more people that harms others based on their sexual or gender identity, or by enforcing harmful gender norms. This action is carried out using the internet and/or mobile technology and includes stalking, bullying, sexual harassment, defamation, hate speech and exploitation” - **International Center for Research on Women (ICRW).**

L’esito dei lavori dell’*Expert Group* di cui sopra ha prodotto una convincente definizione di **TFVAWG** - richiamata in un recente studio di *UN Women* (*Technology-facilitated violence against women: Report of the foundational meeting of the expert group*, marzo 2023):

“any act that is committed, assisted, aggravated or amplified by the use of ICTs or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political or economic harm, or other infringements of rights and freedoms”.

In questa definizione, come emerge, non troviamo alcuna elencazione di fattispecie-tipo perché ciò, secondo gli esperti, garantirebbe una ‘resistenza al tempo’ della stessa (c.d. *time-invariant definition*).

## ELEMENTI-CHIAVE CHE CARATTERIZZANO LE DIVERSE FORME DI TFVAWG

- **dimensione di genere di questa violenza e motivazione dell'atto -** gli atti di cui trattasi si rivolgono in modo diretto contro le donne o in modo sproporzionato contro di esse;
- **'mezzi'** che facilitano questa violenza - il riferimento comune è ovviamente alle *ICTs*, alle tecnologie in generale e/o a tecnologie specifiche, quali ad esempio *spyware* o GPS;
- **'luogo' -** ci si riferisce a questa violenza come 'online' o 'cibernetica' o 'digitale';
- **diverse espressioni della TFVAWG** – sono incluse con elenchi più o meno estesi;
- **danno -** è uno degli elementi che rinveniamo, sia con riferimento al danno in generale che a forme specifiche di danno conseguenti da altrettanto specifiche tipologie di violenza: fisica, sessuale, psicologica, sociale, economica o di altra natura;
- **elemento della continuità** (*continuum*) tra le forme di violenza *online* e *offline* e viceversa - ad esempio, una donna potrebbe essere perseguitata *online* e poi lo *stalker* potrebbe presentarsi sul posto di lavoro, oppure un *partner* che abusa di una donna a casa, può monitorarla e controllare i suoi movimenti fuori casa utilizzando la tecnologia *GPS*

# LE DIVERSE ESPRESSIONI DELLA VIOLENZA DI GENERE *ONLINE* E DI QUELLA C.D. 'TECHNOLOGY -FACILITATED'

- Gli atti persecutori (***cyber stalking***) contro donne e ragazze comportano atti intenzionali ripetuti contro donne e/o ragazze a causa del loro genere o a causa di una combinazione di genere e altri fattori (ad esempio razza, età, disabilità, sessualità, professione o convinzioni personali). Ha lo scopo, attraverso l'uso di mezzi ICT, di molestare, intimidire, perseguitare, spiare o stabilire comunicazioni indesiderate o un contatto, mettendo in atto comportamenti dannosi che facciano sentire la vittima minacciata, angosciata o, in generale, insicura.
- Le molestie informatiche (***cyber harassment***) contro donne e ragazze comportano uno o più atti contro le vittime a causa del loro genere o a causa di una combinazione di genere e di altri fattori (ad esempio razza, età, disabilità, professione, convinzioni personali o orientamento sessuale). Esse si commettono attraverso l'uso di mezzi informatici per molestare, imporre o intercettare comunicazioni, con lo scopo o l'effetto di creare un ambiente intimidatorio, ostile, degradante, umiliante o offensivo per la vittima.

- Per **cyberbullismo** contro le ragazze si intende qualsiasi forma di pressione, aggressione, molestia, ricatto, insulto, denigrazione, diffamazione, furto o acquisizione di identità, trattamento o diffusione illeciti di dati personali, effettuati ripetutamente con mezzi informatici per motivi di genere o di una combinazione di genere e altri fattori (ad esempio razza, disabilità o orientamento sessuale), il cui scopo è isolare, attaccare o deridere un minore o un gruppo di minori.
- L'**uso abusivo/non consensuale di immagini intime** comporta la distribuzione attraverso mezzi ICT o la minaccia di distribuzione attraverso mezzi informatici di immagini/video intimi, privati e/o manipolati di una donna o ragazza senza il suo consenso. Le immagini/video possono essere ottenute in modo non consensuale, manipolati in modo non consensuale o ottenuti in modo consensuale ma distribuiti in modo non consensuale. Le motivazioni comuni includono la sessualizzazione della vittima, l'inflizione di danno alla vittima o l'influenza negativa sulla vita della vittima.

- Tra le peggiori espressioni di violenza di genere *online* emerge, infine, il fenomeno dell'***HATE SPEECH***: esso è giuridicamente complesso in quanto mette in 'crisi' una delle libertà che sono il fondamento di ogni ordinamento democratico, ovvero la libertà di **ESPRESSIONE!!**
- Il **pensiero e la sua esternazione** coinvolgono tanto il profilo della comunicazione privata con altri in condizione di riservatezza, esaurendosi così nell'ambito dei rapporti privati di ciascuno, quanto la dimensione della manifestazione del proprio pensiero a tutti in forma pubblica, producendo così una interazione con il resto della collettività → stretto legame fra la libertà di manifestazione del pensiero e la **democraticità stessa di un sistema** che, garantendo e concretamente attuando il libero confronto fra opinioni, giudizi e convinzioni diverse in campo politico, religioso, culturale, economico, etc., realizza un circuito di comunicazione aperta e trasparente fra società civile e Stato.

- A livello giurisprudenziale, nazionale e sovranazionale, la libertà di espressione è però passibile di limitazioni e viene 'bilanciata' con altri diritti. Questo è, in primo luogo, una conseguenza del fatto che non si tratta di un "diritto assoluto" (c.d. *balancing of interests*).
- L'esigenza di garantire la libertà e il pluralismo dei media e la libertà di espressione di ogni individuo, inclusa la libertà di opinione, possono essere pienamente garantite soltanto nel rispetto delle libertà e dei diritti umani, ovvero tutelando la **dignità della persona**! L'*hate speech*, infatti, va proprio a ledere tale diritto fondamentale…
- Perché ci sia *hate speech* - il quale, secondo i filosofi del linguaggio, ha natura performativa e si caratterizza per essere perlocutorio, in quanto prodromico "all'azione da parte di chi ascolta" - è necessario che concorrano tre elementi:

1. la manifesta volontà di incitare all'odio;
2. un incitamento che sia idoneo a causare atti di odio e violenza;
3. il rischio che tali atti si verifichino…

- Gli **sviluppi tecnologici** hanno favorito le ‘connessioni’, la condivisione di informazioni e idee…hanno perfino rafforzato la nostra capacità di promuovere e difendere i diritti fondamentali…ma sono anche diventati **strumento ‘al servizio’ della violenza contro le donne**, soprattutto contro alcune categorie di donne, in genere quelle che manifestano un’emancipazione rispetto a ruoli precostituiti.
- L'incitamento all'odio *online* basato sul genere (***sexist hate speech***) è definito come un contenuto pubblicato e condiviso tramite le *ICTs* che:

a) **provochi odio nei confronti delle donne e/o delle ragazze** a causa del loro genere o a causa di una combinazione di genere e altri fattori (ad esempio razza, età, disabilità, sessualità, etnia, nazionalità, religione o professione); e/o

b) **diffonda, inciti, promuova o giustifichi l'odio in base al genere**, o a causa di una combinazione di genere e altri fattori (ad esempio razza, età, disabilità, sessualità, etnia, nazionalità, religione o professione).

# L'APPLICAZIONE DEL QUADRO GIURIDICO INTERNAZIONALE IN MATERIA DI DIRITTI UMANI ALLA VIOLENZA DI GENERE *ONLINE*

- Sul piano universale, negli ultimi quindici anni ci sono stati sviluppi significativi nella materia di cui ci stiamo occupando innanzitutto a livello di ***soft law***.
- La questione della violenza di genere *online* è stata infatti affrontata per la prima volta nel **2006** dal Segretario Generale delle Nazioni Unite nel suo nel suo ***In-depth study on all forms of violence against women*** **(A/61/122/Add.1 e Corr.1)**, in cui era emersa la necessità di indagare con attenzione sull'incremento dell'utilizzo delle *ICTs* al fine di intercettare e reprimere sul nascere le forme emergenti di violenza *online* contro le donne.
- In seguito, lo ***Human Rights Council*** nella sua risoluzione ***The promotion, protection and enjoyment of human rights on the Internet*** (20/8 del **2012**), aveva affermato chiaramente che gli stessi diritti di cui le persone godevano *offline* avrebbero dovuto essere tutelati anche *online*. Con questo documento – che ha proposto una visione di Internet e delle tecnologie digitali come qualcosa in grado di promuovere alcuni diritti e dello spazio digitale come 'luogo' in cui 'estendere' il godimento dei diritti detenuti *offline* – si è aperta la strada alla discussione su come le tecnologie digitali avessero iniziato ad avere un impatto importante sui diritti sulle donne e delle ragazze, in particolare proprio con riferimento alla violenza di genere.

- Nel **2013**, nelle sue 'Conclusioni concordate', la *UN Commission on the status of Women* ha invitato gli Stati ad utilizzare le *ICTs* per dare maggiore potere alle donne e, al contempo, a sviluppare meccanismi per combattere la violenza contro donne e ragazze (**E/2013/27**).
- Nello stesso anno, poi, l'**Assemblea Generale**, nella sua **risoluzione 68/181**, è andata oltre esprimendo la sua grave preoccupazione per il fatto che i difensori dei diritti umani delle donne fossero a rischio e subissero violazioni perpetrate sia *online* che *offline* da parte di attori statali e non statali e ha richiamato gli Stati membri ad esercitare la dovuta diligenza e a consegnare tempestivamente i colpevoli alla giustizia.
- Ancora, nel **2015**, lo ***Human Rights Council***, nella sua **risoluzione 29/14**, aveva riconosciuto che la violenza domestica potesse includere atti come il *cyberbullismo* e il *cyberstalking*, che era necessario rafforzare l'inquadramento della violenza di genere *online* come parte del *continuum* della violenza contro le donne e che gli Stati avevano una responsabilità primaria nella prevenzione e nella promozione dei diritti umani delle donne e delle ragazze vittime di violenza.

- Nel **2016**, **l'Assemblea Generale**, nella **risoluzione 71/199**, aveva riconosciuto che le donne erano particolarmente colpite dalle violazioni del diritto alla *privacy* nell'era digitale e aveva invitato tutti gli Stati a sviluppare ulteriormente misure preventive e rimedi adeguati.

- Nel **2017**, è lo ***Human Rights Council***, nella sua **risoluzione 34/7**, a riaffermare questo appello, rilevando che gli abusi del diritto alla ***privacy*** nell'era digitale poteva riguardare tutti gli individui, con effetti particolarmente intensi su alcune categorie più vulnerabili tra cui, appunto, le donne.

- Ancora, nella sua **Raccomandazione n. 35/2017** il **Comitato sulla Convenzione sull'eliminazione di tutte le forme di discriminazione contro le donne** (1979 – Cedaw) ha incluso nella nozione di **'violenza di genere'** anche quella **a carattere virtuale**: in essa, può infatti leggersi che: «[g]ender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private, including in the contexts of the family, the community, public spaces, the workplace, leisure, politics, **sport, health services** and educational settings, and the **redefinition of public and private through technology-mediated environments, such as contemporary forms of violence occurring online and in other digital environments**» (par. 20).

- Nel **2018**, il già menzionato ***Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on online violence against women and girls from a human rights perspective***, ricordava poi che sebbene le forme di violenza *online* si stessero evolvendo, non si trattava però di un fenomeno del tutto nuovo, anzi.

- L'**Assemblea generale delle Nazioni Unite** è tornata anche nel **2020** a prendere una posizione molto netta contro la violenza di genere, anche nella sua dimensione digitale/tecnologia con le sue ***Risoluzioni sull'intensificazione degli sforzi per prevenire ed eliminare tutte le forme di violenza nei confronti di donne e ragazze*** e ***sul diritto alla tutela della vita privata nell'era digitale***, adottate entrambe il **16 dicembre 2020**. In particolare, in quest'ultima si è evidenziato che «the promotion of and respect for the right to privacy are important to the prevention of violence, including gender-based violence, abuse and sexual harassment, in particular against women and children, as well as any form of discrimination, which can occur in digital and online spaces and includes cyberbullying and cyberstalking» (p. 2): emerge, dunque, in tutta la sua evidenza il rapporto tra azioni volte a impedire violazioni del diritto alla tutela della vita privata (anche) delle donne e conseguente effetto preventivo rispetto a possibili aggressioni **online**.

- Più di recente, il ***Secretary-General's report to UNGA77 on the intensification of efforts to eliminate all forms of violence against women and girls***, diffuso nel **settembre 2022**, si è specificatamente concentrato sul bisogno oltremodo urgente di affrontare la violenza contro le donne e le ragazze nel contesto digitale, così come sulla necessità di ampliare gli sforzi per eradicare tutte le forme di violenza contro le donne.

- Da ultimo, il **20 marzo 2023** la ***Commission on the Status of Women*** (CSW), al termine della sua 67ima sessione, ha presentato le sue 'agreed conclusions' dedicate proprio al tema **"Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls"**.

# ATTI VINCOLANTI

- *Rationae materiae* occorre partire dalla ***Convenzione sull'eliminazione di ogni forma di discriminazione contro le donne*** del 1979. Sebbene essa preceda sia l'avvento di Internet che lo sviluppo delle *ICTs* come le conosciamo oggi, la sua 'attualizzazione' è però avvenuta grazie all'opera del Comitato EDAW.
- Ad esempio, nella sua ***Raccomandazione generale n. 33 del 2015 sull'accesso delle donne alla giustizia***, esso ha riconosciuto l'importante ruolo degli spazi digitali e delle *ICTs* per l'emancipazione delle donne. Inoltre, nella già menzionata ***Raccomandazione generale n. 35 del 2017 sulla violenza di genere contro le donne***, il Comitato ha chiarito che la Convenzione era pienamente applicabile ai 'technology-mediated environments' come luoghi in cui spesso possono avere luogo queste forme contemporanee di violenza contro le donne e le ragazze.

- Inoltre, nella ***Raccomandazione generale n. 34 del 2016 sui diritti delle donne rurali***, il Comitato aveva messo in evidenza anche alcuni aspetti positivi del rapporto donne/nuove tecnologie: esso, infatti, aveva evidenziato l'importante ruolo svolto delle *ICTs* sia nella trasformazione degli stereotipi di tipo sociale e culturale che colpiscono le donne che nel potenziamento delle garanzie relative a un più efficace ed efficiente accesso alla giustizia.
- Ancora, nella sua ***Raccomandazione generale n. 36 del 2017 sul diritto delle ragazze e delle donne all'istruzione***, il Comitato ha anche riconosciuto le conseguenze subiscono le ragazze vittime di atti di cyberbullismo, in particolare in relazione al loro diritto all'istruzione. A tal proposito, nel riconoscere il potenziale che le *ICTs* e i *social media* hanno nel promuovere anche un maggiore accesso all'informazione e all'istruzione, gli Stati dovrebbero sviluppare e attuare programmi educativi, anche globali, che puntino a potenziare la consapevolezza e la cultura dei diritti umani delle donne.

In relazione agli abusi *online*, molto interessante e importante è la recente ***Convenzione OIL n. 190 del 2019 sulla violenza e le molestie nel mondo del lavoro***, ratificata in Italia il 29 ottobre 2021 ed entrata in vigore sul piano internazionale il 25 giugno 2021 e la relativa **Raccomandazione n. 206** (il 18 settembre 2023 il Consiglio dell'unione europea ha adottato la sua posizione sulla *Draft Decision* con la quale l'Unione europea invita tutti gli Stati membri a ratificare la Convenzione).

La violenza e le molestie sul lavoro sono purtroppo un fenomeno diffuso e persistente in tutto il mondo: più di una persona su cinque, infatti, ha subito violenze e molestie sul lavoro, siano esse fisiche, psicologiche o sessuali, e le donne sono particolarmente a rischio.

La Convenzione fornisce un quadro comune per prevenire, porre rimedio ed eliminare la violenza e le molestie nel mondo del lavoro, comprese la violenza e le molestie basate sul genere.

Per la prima volta nel diritto internazionale, viene specificamente riconosciuto il diritto di ognuno a un mondo del lavoro libero dalla violenza e dalle molestie, compreso l'obbligo di rispettare, promuovere e realizzare tale diritto.

Tale Convenzione, inoltre, contiene la prima definizione internazionale di violenza e molestie nel mondo del lavoro: "**Articolo 1** - 1. Ai fini della presente Convenzione: a) l'espressione "violenza e molestie" nel mondo del lavoro indica un insieme di pratiche e di comportamenti inaccettabili, o la minaccia di porli in essere, sia in un'unica occasione, sia ripetutamente, che si prefiggano, causino o possano comportare un danno fisico, psicologico, sessuale o economico, e include la violenza e le molestie di genere; b) l'espressione "violenza e molestie di genere" indica la violenza e le molestie nei confronti di persone in ragione del loro sesso o genere, o che colpiscano in modo sproporzionato persone di un sesso o genere specifico, ivi comprese le molestie sessuali. […]".

All’**art. 3 (d)** si afferma che essa si applica «alla violenza e alle molestie nel mondo del lavoro che su verifichino in occasione di lavoro, in connessione con il lavoro o che scaturiscano dal lavoro: […] d) a seguito di comunicazioni di lavoro, incluse quelle rese possibili dalle tecnologie dell’informazione e della comunicazione. […]».

Anche gli ‘ambienti digitali’, dunque, vengono chiaramente identificati come ‘luoghi di lavoro’ nei quali violenze e molestie possono avere luogo nei confronti delle donne, che abbiamo visto esserne maggiormente colpite.

La *cyber*-violenza e quella facilitata dalle nuove tecnologie non solo violano, come abbiamo visto, il **diritto alla non discriminazione** delle donne ma hanno un impatto drammatico su altri diritti quali quello alla ***privacy***.

Esso, invero, così come riconosciuto dall'**art. 12 della Dichiarazione Universale dei Diritti umani** e **art. 17 del Patto internazionale sui diritti civili e politici**, è stato messo in discussione dallo sviluppo delle *ICTs* e degli ambienti digitali.

In un rapporto su ***The Right to Privacy*** del 25 ottobre 2018, il ***Relatore Speciale sul diritto alla privacy*** aveva evidenziato la necessità di esaminare la violenza informatica contro i soggetti più vulnerabili, compresa la violenza domestica resa possibile o facilitata dai dispositivi digitali (**A/HRC/37/62**).
Con la raccolta e l'archiviazione sempre più massiccia di dati da parte di intermediari e altre aziende, la tutela della *privacy* è oggi fondamentale. Già nel **2013** però, l'Assemblea Generale aveva espresso profonda preoccupazione per l'impatto negativo che, ad esempio, l'intercettazione delle comunicazioni poteva avere sui diritti umani (**risoluzione 68/167**).

Strumenti importanti per proteggere la *privacy* sono sia la crittografia che l'anonimato, separatamente o insieme: essi facilitano la libertà di espressione nel rispetto della *privacy* in quanto garantiscono la riservatezza mentre si facilita la libertà di cercare, ricevere e diffondere informazioni e idee.

L'anonimato *online* gioca poi un ruolo importante per le donne e gli altri soggetti a rischio di stigmatizzazione in quanto consente loro di cercare informazioni, trovare solidarietà, sostegno e condivisione di opinioni senza timore di essere identificati (vedi ***Report of the Special Rapporteur on the promotion andprotection of the right to freedom of opinion and expression, David Kaye, on encryption, anonymity, and the human rights framework*** - A/HRC/29/32).

# IL CONTESTO REGIONALE EUROPEO

- L'impegno del **Comitato dei Ministri del Consiglio d'Europa** rispetto al contrasto di una delle concause delle condotte di cui ci stiamo occupando, ovvero il **sessismo**, anche nelle sue manifestazioni *online*, si è specificamente concretizzato nell'adozione nel **2019** della ***Raccomandazione sulla prevenzione e la lotta al sessismo***. Il primo aspetto che rileva è l'inclusione di una definizione condivisa di 'sessismo', che include ogni atto, gesto, rappresentazione visiva, proposta orale o scritta, pratica o comportamento – fondato sull'idea che una persona o un gruppo di persone siano inferiori per via del loro genere – che si verificano nella sfera pubblica o privata, *online* oppure *offline*.
- Tali condotte comportano o hanno come effetto la **violazione della dignità** o dei diritti fondamentali di una persona o di un gruppo di persone e provocano danni o sofferenze di natura fisica, sessuale, psicologica o socio-economica. Inoltre, esse possono **contribuire a creare un ambiente intimidatorio, ostile, mortificante, umiliante o offensivo**, ostacolando così l'autonomia e la piena realizzazione dei diritti umani di una persona o di gruppo di persone. Infine, come ovvia conseguenza, il sessismo **mantiene e rafforza gli stereotipi di genere**.

- La Raccomandazione, poi, si sofferma su diversi ambiti entro i quali si possono manifestare atteggiamenti e discorsi sessisti, focalizzandosi proprio sul sessismo in rete che viene definito **'endemico' in tutto il continente europeo** e che colpisce in modo sproporzionato alcune categorie femminili es. giornaliste).

- Quanto alle richieste avanzate nei confronti dei Paesi membri del Consiglio d'Europa, la Raccomandazione prevede che negli ordinamenti statali accanto a **misure di tipo squisitamente sanzionatorio** – come l'introduzione di norme che definiscano e puniscano alla stregua di reati i casi di discorso d'odio sessista – ve ne siano altre ispirate alla logica della centralità dei percorsi virtuosi di **prevenzione**, fondati sull'educazione e sulla sensibilizzazione di possibili vittime e, in generale, degli utenti della rete.

## NORME VINCOLANTI SPECIFICHE

**- Convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica** – meglio conosciuta come **Convenzione di Istanbul** perché finalizzata e firmata in quella città l'11 maggio 2011 (entrata in vigore 1° agosto 2014)

**- Convenzione del Consiglio d'Europa sulla criminalità informatica** (c.d. **Convenzione di Budapest**; adottata il 23 novembre 2001 ed entrata in vigore il 1° luglio 2004).

La **Convenzione di Istanbul**:

- riconosce la violenza sulle donne come una violazione dei diritti umani e come un atto di discriminazione
- è il primo strumento giuridicamente vincolante che definisce specifiche forme di violenza e dispone diversi tipi di protezione per le donne
- può essere ratificata anche da Paesi che non appartengono al Consiglio d'Europa e dall'Unione europea.

La convenzione enuncia chiaramente che la violenza contro le donne e la violenza domestica non possono più essere considerate una questione privata ma che gli Stati hanno un obbligo, dotandosi di politiche globali e integrate, di prevenire la violenza, proteggere le vittime e punirne gli autori.

Ratificando la convenzione, i governi sono obbligati a cambiare le loro leggi, introdurre misure pratiche e stanziare risorse per adottare un approccio di tolleranza zero nei confronti della violenza contro le donne e della violenza domestica. Prevenire e combattere tale violenza non è più una questione di buona volontà ma un obbligo giuridico.
Questo aiuterà le vittime in tutta Europa e in altri Paesi.

Oltre agli obblighi giuridici, la convenzione invia anche un segnale politico forte alla società che la violenza nei confronti delle donne e la violenza domestica sono inaccettabili. La sua ambizione è mettere in luce la realtà di molte donne e ragazze che subiscono violenza, sensibilizzare il pubblico e cambiare le mentalità nel lungo termine.

La Convenzione di Istanbul si fonda su **4 pilastri** per la sua applicazione:

- **Prevenzione**: sensibilizzazione, scuola, formazione, programmi per autori di violenza, partecipazione dei media e del settore privato;
- **Protezione**: informazione alle vittime, servizi generici, servizi specializzati di cui CAV, CR, Linee telefoniche d'aiuto, supporto alle vittime di violenza sessuale, supporto ai/alle minori vittime di violenza assistita, *status* di residente per donne migranti, richiesta d'asilo basata sul genere, divieto di non refoulement. Chiede che si faccia un lavoro di supporto e di *empowerment* con le donne che hanno un vissuto di violenza;
- **Punizione dell'autore di violenza/Compensazione della vittima**: risposte immediate di prevenzione e protezione, valutazione e gestione del rischio, misure urgenti di allontanamento e ordinanze di protezione, indagini e prove, procedimenti di parte ed *ex officio*, misure di protezione, gratuito patrocinio, prescrizione;
- **Politiche integrate**: politiche coordinate e integrate, risorse finanziarie, organizzazioni della società civile delle donne e per i diritti umani, organismi di coordinamento/*governance*, raccolta dati sulla prevalenza della violenza e dati amministrativi, ricerca.

L’altro importante strumento menzionato è, appunto, la **Convenzione sulla criminalità informatica**: si tratta di un trattato incentrato sul contrasto alla criminalità informatica e sulla gestione delle prove elettroniche.

Richiede agli Stati parte di criminalizzare condotte commesse contro o per mezzo di dati e sistemi informatici, ivi comprese quelle consistenti nella produzione, distribuzione o possesso di materiale pedopornografico.

Le parti della convenzione sono, inoltre, tenute a stabilire poteri e procedure per garantire la sicurezza delle prove elettroniche acquisite ai fini di specifiche indagini penali, non solo per i reati di cui sopra, ma anche per qualsiasi reato in cui le prove siano in formato elettronico, e per facilitare efficacemente la cooperazione internazionale e l’assistenza giudiziaria reciproca in materia di indagini penali o procedimenti relativi a tali crimini.

La Convenzione è completata da **un Protocollo addizionale sulla xenofobia e il razzismo commessi attraverso sistemi informatici** del novembre 2002, entrato in vigore il 1° marzo 2006 e da un **Secondo protocollo addizionale volto a rafforzare la cooperazione e la divulgazione delle prove elettroniche**, adottato il 12 maggio 2022 e non ancora in vigore.

Il Comitato per la Convenzione sulla criminalità informatica (T-CY) garantisce poi l'efficace attuazione della Convenzione e dei suoi Protocolli aggiuntivi.

La **Convenzione di Budapest** attraverso una serie di norme di diritto penale sostanziale affronta direttamente e indirettamente alcuni tipi di violenza *online* e facilitata dalla tecnologia contro le donne. Altre disposizioni riguardano atti che agevolano questo tipo di violenza. Rilevanti sono pure le disposizioni sui poteri procedurali e sulla cooperazione internazionale e ai fini delle attività di investigazione e di messa in sicurezza delle prove elettroniche.

Gli **articoli 33, 34 e 40 della Convenzione di Istanbul** coprono un gran numero di forme di violenza perpetrabili anche *online* o attraverso l'uso delle nuove tecnologie.

Partendo dalle **molestie sessuali**, esse sono richiamate nell'**art. 40**: "Le Parti adottano le misure legislative o di altro tipo necessarie per garantire che qualsiasi forma di comportamento indesiderato, verbale, non verbale o fisico, di natura sessuale, con lo scopo o l'effetto di violare la dignità di una persona, segnatamente quando tale comportamento crea un clima intimidatorio, ostile, degradante, umiliante o offensivo, sia sottoposto a sanzioni penali o ad altre sanzioni legali".

A fronte di questa norma che 'criminalizza' tali condotte, vi sono poi delle norme della **Convenzione di Budapest** che 'aiutano' nel rafforzamento della tutela: **Articolo 2 - Accesso illegale ad un sistema informatico**: "Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per sanzionare come reato in base alla propria legge nazionale l'accesso all'intero sistema informatico o a parte di esso senza autorizzazione. Una Parte può richiedere che il reato venga commesso violando misure di sicurezza con l'intenzione di ottenere informazioni all'interno di un computer o con altro intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico"

**Articolo 3 - Intercettazione abusiva**: “Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale l'intercettazione senza autorizzazione, fatta con strumenti tecnici, di trasmissioni non pubbliche di dati informatici a, da o all'interno di un sistema informatico, incluse le emissioni elettromagnetiche da un sistema informatico che ha tali dati informatici.

Una Parte può richiedere che il reato venga commesso con intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico”.

**Articolo 6 - Abuso di apparecchiature:** “1 Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commessi intenzionalmente e senza autorizzazione:
a. la fabbricazione, la vendita, l’approvvigionamento per l’uso, l’importazione, la distribuzione o l’utilizzabilità in altro modo di: 1. un’apparecchiatura, incluso un programma per computer, destinato o utilizzato principalmente al fine di commettere un qualsiasi reato in base agli articoli da 2 a 5 di cui sopra; 2. una password di un computer, un codice d’accesso, o informazioni simili con le quali l'intero sistema informatico o una sua parte sono accessibili, con l’intento di commettere qualsiasi reato in base agli articoli da 2 a 5 di cui sopra; b. il possesso di un elemento di cui ai sopra citati paragrafi a. 1. o 2., con l’intento di utilizzarlo allo scopo di commettere qualche reato in base agli articoli da 2 a 5. Una Parte può richiedere per legge che vi sia il possesso di un certo numero di tali elementi perché vi sia una responsabilità penale. […]”.

**Articolo 8 - Frode informatica:** “Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesso intenzionalmente e senza alcun diritto, il cagionare un danno patrimoniale ad altra persona: a. con ogni introduzione, alterazione, cancellazione o soppressione di dati informatici; b. con ogni interferenza nel funzionamento di un sistema informatico, con l’intento fraudolento o illegale di procurare, senza alcun diritto, un beneficio economico per se stesso o altri”.

**Articolo 10 – Reati contro la proprietà intellettuale e diritti collegati**: “1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale la violazione della proprietà intellettuale, […], con l’eccezione di tutti i diritti morali conferiti da queste convenzioni, se tali atti sono commessi deliberatamente, su scala commerciale e attraverso l’utilizzo di un sistema informatico”.

**Quanto allo *stalking online*, nella Convenzione gli atti persecutori** sono richiamati dall'**art. 34:** "Le Parti adottano le misure legislative o di altro tipo necessarie per penalizzare un comportamento intenzionalmente e ripetutamente minaccioso nei confronti di un'altra persona, portandola a temere per la propria incolumità". Nel rapporto esplicativo, invero, si delinea ulteriormente questa condotta e si includono anche le modalità di perpetrazione attraverso le ICTs: "Il comportamento minaccioso può consistere nel seguire ripetutamente un'altra persona, attivare comunicazioni indesiderate con un'altra persona o farle sapere che viene osservata. Tale comportamento include anche l'inseguimento fisico della vittima, il presentarsi sul posto di lavoro, di sport o di istruzione, nonché il perseguitare la vittima nel mondo virtuale (*chat room*, siti di *social network*, ecc.). Instaurare una comunicazione indesiderata implica il perseguimento di qualsiasi contatto attivo con la vittima con tutti i mezzi di comunicazione disponibili, compresi i moderni strumenti di comunicazione e le *ICTs*".

Anche in questo caso, poi, ulteriore supporto arriva da alcune disposizioni della Convenzione di Budapest, in particolare dagli **artt. 2-6.**

Le condotte di cui ci stiamo occupando possono essere anche qualificabili alla stregua di **violenza psicologica**.

Questa è contemplata dall'**art. 33** della Convenzione di Istanbul: "Le Parti adottano le misure legislative o di altro tipo necessarie per penalizzare un comportamento intenzionale mirante a compromettere seriamente l'integrità psicologica di una persona con la coercizione o le minacce".

In relazione alla Convenzione di Istanbul che, di per sé, non aveva norme specifiche sulla violenza online/technology-facilitated, dobbiamo necessariamente richiamare la **Raccomandazione generale n. 1 sulla dimensione digitale della violenza sulle le donne** del **GREVIO** (Gruppo di esperti sulla lotta contro la violenza nei confronti delle donne e la violenza domestica), adottata il **20 ottobre 2021**. Nella sua attività di monitoraggio della Convenzione di Istanbul, il GREVIO ha invero rilevato che la dimensione digitale della violenza contro le donne viene spesso trascurata dalle leggi e le politiche nazionali.

Nella nuova Raccomandazione è stata introdotta la definizione **"dimensione digitale della violenza sulle donne",** che comprende sia gli atti di violenza perpetrati *online* – condividere immagini umilianti, insulti, minacce di morte e di stupro – sia atti di violenza compiuti utilizzando tecnologie esistenti e non ancora inventate – come tecnologie di tracciamento riportate dalle società di sicurezza informatica.

# …E LA CEDU?

- La **Corte europea dei diritti dell'uomo** è intervenuta in materia di cyberviolenza con la sentenza resa nel caso ***Buturugă c. Romania*** dell'**11 febbraio 2020** (ricorso n. 56867/15). La CEDU ha ritenuto che la cyberviolenza deve essere considerata come una forma di violenza contro le donne e, di conseguenza, le autorità nazionali non possono trattare episodi come **l'utilizzo abusivo degli *account* di una donna da parte dell'ex marito o l'acquisizione di immagini e dati** come casi di violenza ordinaria, ma devono prevedere l'applicazione delle regole più stringenti fissate per i casi di violenza domestica. La Corte ha qui precisato che la violenza contro le donne non è solo quella fisica, ma include anche la violenza psicologica, nonché lo *stalking* e la *cyberviolenza*.
- Pertanto, dagli **artt. 3** (divieto di trattamenti inumani e degradanti) **e 8** (diritto al rispetto della vita privata, che include quello alla riservatezza della corrispondenza) **CEDU** deriva l'obbligo positivo di adottare misure preventive e sanzionatorie nei casi in cui una donna subisca intrusioni nel proprio computer, nei profili sui social, nonché furti di dati personali intimi e immagini.

A rivolgersi alla Corte è stata una cittadina rumena che aveva depositato una denuncia contro il marito per i ripetuti episodi di violenza domestica e per l'utilizzo abusivo, da parte dell'ex marito, dei suoi account, inclusa la sua pagina Facebook, l'intromissione nel computer, lo stalking via web e l'acquisizione di dati e immagini. Il procuratore aveva archiviato queste denunce perché i comportamenti dell'uomo non erano stati considerati come "particolarmente gravi". La decisione era stata impugnata dalla donna e il tribunale di primo grado aveva disposto una misura di protezione applicabile per 6 mesi che, però, non era stata eseguita in modo effettivo.

Prima di tutto, la Corte europea ha chiarito che i casi di violenza domestica devono essere trattati in modo diverso rispetto alle altre forme di violenza, in linea con la Convenzione di Istanbul e ha respinto la tesi sostenuta dalle autorità nazionali circa la non "sufficiente gravità" dei fatti e la "debolezza" nella reazione della stessa vittima che avrebbe avuto un comportamento poco diligente – anche sotto il profilo della tempistica – nella presentazione delle denunce. Per la Corte europea, infatti, le autorità nazionali non hanno considerato l'impatto psicologico di queste forme di violenza sulle donne e il senso di isolamento che spinge le vittime a ritirare le denunce.

Pertanto, anche in presenza di un quadro normativo interno idoneo, per Strasburgo si verifica una violazione della Convenzione in assenza di misure effettive. **Non è sufficiente, infatti, adottare un ordine di protezione se poi non è garantita l'applicazione effettiva della misura.**

# *SEGUE*. L'AZIONE DELL'UNIONE EUROPEA

- Il **Regolamento generale sulla protezione dei dati adottato dall'Unione Europea** (GDPR, **27 aprile 2016**, in vigore dal 25 maggio 2018) richiede, tra le altre cose, alle aziende di attuare misure ragionevoli di protezione dei dati per proteggere i dati personali e la *privacy* dei consumatori contro la perdita o l'esposizione dei dati. Esso è molto importante anche perché afferma il principio dell'extraterritorialità della giurisdizione, dato che è applicabile a tutte le società dell'Unione europea e alle società extra UE che raccolgono o trattano dati personali di soggetti residenti nell'Unione.
- **Regolamento (UE) 2022/2065 del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali** e che modifica la direttiva 2000/31/CE (c.d. **Digital Services Act**) del 19 ottobre 2022 che si applicherà a decorrere dal **17 febbraio 2024**.

Alla fine del 2020 la Commissione europea aveva proposto una riforma orizzontale della disciplina europea in materia di responsabilità delle piattaforme per diffusione di contenuti illeciti, il c.d. *Digital Services Act*, consistente in una serie di norme sugli obblighi e la responsabilità degli **intermediari digitali** all'interno del mercato unico: queste, invero, sono graduate in funzione della dimensione degli operatori e della conseguente capacità di conoscenza dei contenuti che vengono caricati dagli utenti.

Esso prevede **nuove procedure per conseguire una più rapida rimozione dei contenuti illegali e una protezione globale dei diritti fondamentali degli utenti *online*.** Il suo impatto nello spazio digitale europeo sarà notevole in quanto si tratta di un atto vincolante che ha il pregio di promuovere un riequilibrio tra i diritti e le responsabilità degli utenti, delle piattaforme di intermediazione e delle autorità pubbliche e si basa sui valori europei, compresi il rispetto dei diritti umani, la libertà, la democrazia, l'uguaglianza e lo Stato di diritto.

In particolare, ai sensi dell'**art. 34** del **Regolamento**, relativo alla **valutazione del rischio**, la violenza di genere rientra tra i 'rischi sistemici' cui bisogna prestare massima attenzione. A tal fine si dispone che "I fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca *online* di dimensioni molto grandi individuano, analizzano e valutano con **diligenza** gli eventuali **rischi sistemici** nell'Unione derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi. […] La **valutazione del rischio** deve essere specifica per i loro servizi e proporzionata ai **rischi sistemici**, tenendo in considerazione la loro gravità e la loro probabilità, e deve comprendere i seguenti rischi sistemici: a) la diffusione di **contenuti illegali** tramite i loro servizi; b) eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, in particolare i diritti fondamentali alla **dignità umana** sancito nell'articolo **1** della Carta, al **rispetto della vita privata e familiare** sancito nell'articolo **7** della Carta, alla **tutela dei dati personali** sancito nell'articolo **8** della Carta, alla **libertà di espressione e di informazione**, inclusi la libertà e il pluralismo dei media, sanciti nell'articolo **11** della Carta, e alla **non discriminazione** sancito nell'articolo **21** della Carta, al **rispetto dei diritti del minore** sancito nell'articolo **24** della Carta, così come all'elevata tutela dei consumatori, sancito nell'articolo **38** della Carta; c) eventuali effetti negativi, attuali o prevedibili, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica; d) qualsiasi effetto negativo, attuale o prevedibile, in relazione alla **violenza di genere**, alla protezione della salute pubblica e dei minori e alle **gravi conseguenze negative per il benessere fisico e mentale della persona**".

A questa importante attività di valutazione *ex ante*, il Regolamento ne affianca una di tipo squisitamente preventivo. Il successivo **art. 35** infatti, rubricato **'Attenuazione dei rischi'** prevede che "1. I fornitori di piattaforme *online* di dimensioni molto grandi e di motori di ricerca *online* di dimensioni molto grandi adottano misure di attenuazione ragionevoli, proporzionate ed efficaci, adattate ai **rischi sistemici specifici** individuati a norma dell'articolo 34, prestando particolare attenzione agli **effetti di tali misure sui diritti fondamentali**. Tali misure possono comprendere, ove opportuno: a) l'adeguamento della progettazione, delle caratteristiche o del funzionamento dei loro servizi, anche delle loro interfacce *online*; b) l'adeguamento delle condizioni generali e la loro applicazione; c) l'adeguamento delle procedure di moderazione dei contenuti, compresa la velocità e la qualità del trattamento delle segnalazioni concernenti tipi specifici di contenuti illegali e, se del caso, la rapida rimozione dei contenuti oggetto della notifica o la disabilitazione dell'accesso agli stessi, in particolare in relazione **all'incitamento illegale all'odio e alla violenza *online***, nonché l'adeguamento di tutti i processi decisionali pertinenti e delle risorse dedicate alla moderazione dei contenuti;

d) la sperimentazione e l’adeguamento dei loro sistemi algoritmici, compresi i loro sistemi di raccomandazione; e) l’adeguamento dei loro sistemi di pubblicità e l’adozione di misure mirate volte a limitare o ad adeguare la presentazione della pubblicità associata al servizio da esse prestato; f) il rafforzamento dei processi interni, delle risorse, della sperimentazione, della documentazione o della vigilanza sulle loro attività, in particolare per quanto riguarda il **rilevamento dei rischi sistemici**; g) l’avvio o l’adeguamento della cooperazione con i segnalatori attendibili in conformità dell’articolo 22 e l'attuazione della decisione degli organismi di risoluzione extragiudiziale delle controversie a norma dell'articolo 21; h) l’avvio o l’adeguamento della cooperazione con altri fornitori di piattaforme *online* o di motori di ricerca *online* attraverso i codici di condotta e i protocolli di crisi di cui rispettivamente agli articoli 45 e 48; i) l’adozione di misure di sensibilizzazione e l’adattamento della loro interfaccia *online* al fine di dare ai destinatari del servizio maggiori informazioni; j) l’adozione di misure mirate per tutelare i diritti dei minori, compresi strumenti di verifica dell’età e di controllo parentale, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno, a seconda dei casi; k) il ricorso a un contrassegno ben visibile per fare in modo che un elemento di un’informazione, sia esso un’immagine, un contenuto audio o video, generati o manipolati, che assomigli notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che a una persona appaia falsamente autentico o veritiero, sia distinguibile quando è presentato sulle loro interfacce *online* e, inoltre, la fornitura di una funzionalità di facile utilizzo che consenta ai destinatari del servizio di indicare tale informazione.

***Proposta di Direttiva del Parlamento europeo e del Consiglio sulla lotta alla violenza contro le donne e alla violenza domestica***, presentata dalla Commissione l'**8 marzo 2022**. Essa concretizza l'impegno della Commissione nel contrasto alla violenza di genere e prevede misure specifiche in relazione alla violenza attraverso le nuove tecnologie.

Innanzitutto, è molto importante l'aver specificato, tra gli obiettivi della Proposta, la circostanza per cui essa **«tiene conto anche di fenomeni recenti non specificamente affrontati dalla Convenzione di Istanbul come la violenza online contro le donne».**

La Commissione, dunque, è pienamente consapevole che con l'utilizzo di Internet e degli strumenti informatici la violenza *online* continua ad aumentare e spesso fa da corollario o precede la violenza subita dalle vittime nella vita *offline*.

Centrale nell'approccio della Commissione è la **politica di prevenzione**, senza la quale anche le misure repressive più dure poco possono fare per sradicare culturalmente e sociologicamente questo odioso fenomeno. In proposito, rileva l'**art. 36** della Proposta, rubricato proprio '**Misure preventive'.** In esso è previsto che "1. Gli Stati membri adottano misure adeguate per prevenire la violenza contro le donne e la violenza domestica. 2. Le misure preventive comprendono campagne di sensibilizzazione e programmi di ricerca e educativi, se del caso messi a punto in cooperazione con le pertinenti organizzazioni della società civile, le parti sociali, le comunità interessate e altri portatori di interessi. 3. Gli Stati membri mettono a disposizione del pubblico informazioni sulle misure preventive, sui diritti delle vittime, sull'accesso alla giustizia e a un difensore e sulle misure di protezione e assistenza disponibili. 4. Un'azione mirata è rivolta ai gruppi a rischio, compresi i minori, in funzione della loro età e maturità, e alle persone con disabilità, tenendo conto delle barriere linguistiche e dei diversi livelli di alfabetizzazione e abilità. Le informazioni per i minori sono formulate in modo consono.

5. Le misure preventive mirano in particolare a **contrastare gli stereotipi di genere** dannosi, a **promuovere la parità tra donne e uomini** e a incoraggiare tutti, compresi gli uomini e i ragazzi, a fungere da modelli di riferimento positivi per agevolare cambiamenti comportamentali in tutta la società, in linea con gli obiettivi della presente direttiva. […] 7. **Le misure preventive riguardano inoltre in modo specifico la violenza *online*.** In particolare gli Stati membri provvedono affinché **le misure educative includano lo sviluppo di competenze di alfabetizzazione digitale, comprese competenze critiche del mondo digitale, per permettere agli utenti di individuare e affrontare i casi di violenza *online*, cercare assistenza e prevenire detta violenza.** Gli Stati membri promuovono la **cooperazione multidisciplinare e tra portatori di interessi, compresi i prestatori di servizi intermediari e le autorità competenti, per elaborare e attuare misure di contrasto alla violenza *online*.** 8. Gli Stati membri provvedono affinché le pertinenti politiche nazionali affrontino la **tematica delle molestie sessuali sul lavoro**. […]".

Da un punto di vista **dell'armonizzazione delle norme penali** sostanziali, la direttiva chiedi agli Stati membri di criminalizzare e rendere perseguibili:

- **la condivisione non consensuale di materiale intimo o manipolato** (**art. 7**): "Gli Stati membri provvedono affinché siano punite come reato le condotte intenzionali seguenti: (a) rendere accessibile a una pluralità di utenti finali, tramite tecnologie dell'informazione e della comunicazione, immagini, video o altro materiale intimo ritraente atti sessuali di un'altra persona **senza il suo consenso**; (b) produrre o manipolare e successivamente rendere accessibile a una pluralità di utenti finali, tramite tecnologie dell'informazione e della comunicazione, immagini, video o altro materiale in modo da far credere che un'altra persona partecipi ad atti sessuali, **senza il consenso dell'interessato**; (c) minacciare i comportamenti di cui alle lettere a) e b) al fine di costringere un'altra persona a compiere un determinato atto, acconsentirvi o astenersi dallo stesso";

- lo ***Stalking online*** (**art. 8**): “Gli Stati membri provvedono affinché siano punite come reato le condotte intenzionali seguenti: (a) assumere persistentemente nei confronti di un’altra persona comportamenti minacciosi o intimidatori tramite tecnologie dell’informazione e della comunicazione, tali da indurla a temere per l’incolumità propria o delle persone a suo carico; (b) sottoporre un’altra persona a sorveglianza continua tramite tecnologie dell’informazione e della comunicazione, **senza il suo consenso o un’autorizzazione legale a tal fine**, per seguirne o monitorarne i movimenti e le attività; (c) rendere accessibile a una pluralità di utenti finali, **tramite tecnologie dell'informazione e della comunicazione**, materiale contenente i dati personali di un’altra persona **senza il suo consenso**, per istigare detti utenti finali ad arrecare un danno fisico o un ingente danno psicologico a tale persona”;

- **le molestie *online*** (**art. 9**): “Gli Stati membri provvedono affinché siano punite come reato le condotte intenzionali seguenti: (a) sferrare un attacco in concorso con terzi nei confronti di un’altra persona, rendendo accessibile a una pluralità di utenti finali materiale minaccioso o ingiurioso tramite tecnologie dell’informazione e della comunicazione, con l’effetto di provocare un ingente danno psicologico a tale persona; (b) partecipare insieme a terzi a un attacco di cui alla lettera a)”;
- **l’Istigazione alla violenza o all’odio *online*** (**art. 10**): “Gli Stati membri provvedono affinché sia punita come reato la condotta intenzionale consistente nell’istigare alla violenza o all’odio nei confronti di un gruppo di persone o di un membro di detto gruppo definito con riferimento al sesso o al genere, diffondendo al pubblico tramite tecnologie dell’informazione e della comunicazione materiale contenente tale istigazione”.

# FOCUS SULL'*ONLINE SEXIST HATE SPEECH*

Stando al Consiglio d'Europa, questa pratica può essere definita come «one of the expressions of sexism, which can be defined as any supposition, belief, assertion, gesture or act that is aimed at expressing contempt towards a person, based on her or his sex or gender, or to consider that person as inferior or essentially reduced to her or his sexual dimension» (2016) .
Essa, inoltre, non è solo strettamente connessa alla libertà di espressione, ma incide sul rispetto del divieto di discriminazione in base al sesso e sul contrasto alla violenza di genere.
Il **diritto internazionale** non solo non offre alcuna protezione ai **messaggi di incitamento all'odio o alla discriminazione**, ma chiede interventi volti a prevenire e ad arginare la diffusione di detti messaggi, che diventano ancora più pericolosi per la democrazia, quando la diffusione avviene attraverso i *social media*, compromettendo altri diritti umani oggetto di tutela sul piano internazionale come la **dignità della persona.**
A livello di ***soft law***, rileva innanzitutto la **Dichiarazione universale dei diritti dell'uomo del 9 dicembre 1948**, nella quale è garantita la tutela da ogni discriminazione e «contro qualsiasi incitamento a tale discriminazione» (**art. 7**); tra le **fonti vincolanti**, invece, emerge innanzitutto la **Convenzione sull'eliminazione di ogni forma di discriminazione razziale del 21 dicembre 1965**, nella quale è precisato che gli Stati devono punire «ogni propaganda ed ogni organizzazione che s'ispiri a concetti ed a teorie basate sulla superiorità di una razza o di un gruppo di individui di un certo colore o di una certa origine etnica, o che pretendano di giustificare o di incoraggiare **ogni forma di odio** e discriminazione razziale» (**art. 4**), adottando, a tal fine, anche misure positive.

Un espresso divieto di incitamento all'odio è stato inserito nel **Patto sui diritti civili e politici del 16 dicembre 1966**: l'**art. 20**, infatti, impone agli Stati di vietare nell'ordinamento interno «qualsiasi appello all'odio nazionale, razziale o religioso che costituisca incitamento alla discriminazione, all'ostilità o alla violenza». Sul piano applicativo, in diverse occasioni, il Comitato dei diritti umani delle Nazioni Unite non ha accordato una protezione della libertà di espressione quando questa ha riguardato discorsi discriminatori.

Diversamente, la **Convenzione per l'eliminazione di tutte le forme di discriminazione contro le donne (CEDAW) del 1979**, pur imponendo agli Stati di intraprendere misure volte ad eliminare "pregiudizi e stereotipi basati sulla convinzione dell'inferiorità o della superiorità dell'uno o dell'altro sesso", non prevede norme specifiche volte a contrastare l'istigazione all'odio contro le donne.

Di recente, rileva pure la già menzionata **Convenzione OIL n. 190 del 2019 e in particolare il già richiamato art. 3 (d).**

- A livello regionale europeo un ruolo centrale è rivestito dal **Consiglio d'Europa** e, in particolare dalla giurisprudenza relativa alla CEDU, perché se è vero che manca, a differenza del Patto sui diritti civili e politici, una norma *ad hoc* che vieti l'incitamento all'odio è anche vero che la Corte di Strasburgo, tenendo conto che la Convenzione è uno strumento vivente, ha fornito un contributo fondamentale nell'escludere dal perimetro di applicazione **dell'art. 10 della Convenzione europea sui diritti dell'uomo e le libertà fondamentali del 1950**, che assicura la libertà di espressione, le opinioni con finalità discriminatorie e i messaggi di odio in quanto contrastanti con i principi e i valori in essa affermati. Lo stesso art. 10, d'altra parte, richiede che siano poste limitazioni alla libertà di espressione se necessarie in una società democratica, proprio perché la libertà di espressione comporta doveri e responsabilità.

- Se, nei casi più gravi, la Corte ha applicato l'**art. 17 (divieto di abuso di diritto)**, negli altri ha imposto agli Stati un bilanciamento tra il diritto alla libertà di espressione (art. 10) e altri diritti garantiti dalla Convenzione: la libertà di espressione non può essere utilizzata come 'mezzo' per violare altre libertà e diritti, tra cui in particolare la **dignità dell'individuo.**

- Gli Stati, quindi, sono tenuti a vigilare che nell'esercizio della libertà di espressione non si oltrepassino certi limiti anche con riguardo alla reputazione e a diritti altrui. Sulla questione del bilanciamento dei diritti in gioco e sulla valutazione della necessarietà di una misura in una società democratica per giustificare un'ingerenza nell'esercizio di un diritto è centrale la Corte EDU.

In numerosi casi, in cui i ricorrenti lamentavano la lesione della propria libertà di parola a causa di normative nazionali volte a reprime i discorsi d'odio, la Corte non ha riscontrato la violazione dell'art. 10 CEDU, ritenendo al contrario necessario "sanzionare e prevenire la diffusione di espressioni che incitano, promuovono, giustificano l'odio fondato sull'intolleranza", purché tali restrizioni siano "proporzionate allo scopo perseguito" (***Erbakan v. Turkey***, 2006), tanto è vero che "le leggi volte a contrastare il linguaggio dell'odio e a reprimere atti ispirati dal razzismo e dalla xenofobia, rappresentano – in una **società democratica** – una limitazione legittima della libertà di espressione in favore della tutela necessaria della reputazione degli individui e delle libertà fondamentali" (cfr. Corte ***Edu Gündüz v. Turquie***, 2006; *Feret v. Belgium*, 2009).

Complessivamente, i dati giurisprudenziali della Corte sono chiari: analizzando la giurisprudenza in tema di discorso d'odio *online* o *offline*, pur trattandosi di casi molto diversi fra loro, emerge chiaramente come **la Corte consideri l'*hate speech* una violazione dei valori fondamentali della Convenzione.**

Di conseguenza misure legislative nazionali volte a reprimere simili condotte non si pongono in contrasto con l'art. 10 CEDU, purché esse siano proporzionate allo scopo perseguito.

Inoltre, **a partire dal 2015** sono sempre più i casi che coinvolgono commenti sui *social network* e su internet, toccando il delicato tema della responsabilità dei gestori delle piattaforme.

La prima sentenza in materia è stata ***Delfi AS v. Estonia*** del **2015** con la quale la Corte europea ha ritenuto inammissibile il ricorso di un rappresentante di un portale web di informazione condannato per diffamazione a causa della diffusione di commenti offensivi e incitanti all'odio sulla propria pagina.

La condanna per diffamazione del gestore del portale non costituisce, secondo la Corte, una violazione della libertà di manifestazione del pensiero poiché il gestore non ha intrapreso alcuna misura volta a rimuovere i commenti che mettono a rischio i diritti e l'integrità fisica altrui. Nel sistema convenzionale, infatti, l'esercizio della libertà di manifestazione del pensiero comporta doveri e responsabilità cui sono sottoposti anche i gestori delle piattaforme internet.

Un altro caso rilevante è poi quello alla base della sentenza del **2021, *Sanchez v. France***, nella quale la Corte ha confermato la compatibilità con l'art. 10 CEDU di sanzioni pecuniarie a carico di individui che non cancellano tempestivamente i commenti d'odio pubblicati da altri sulle loro bacheche Facebook .

In generale, dunque, dalla giurisprudenza della Corte in tema di discorso d'odio emerge il riconoscimento del contrasto tra *hate speech* e valori fondamentali della Convenzione.

Oltre alla giurisprudenza evolutiva della Corte europea dei diritti dell'uomo, occorre richiamare una serie rilevante di atti di *soft law*.

Si pensi, ad esempio, alla **Raccomandazione 97/20 del Comitato dei Ministri**, adottata nel **1997**, ai sensi della quale l'*hate speech* consiste in quelle espressioni che "[…] diffondono, incitano, promuovono o giustificano l'odio razziale, la xenofobia, l'antisemitismo o altre forme di minaccia basate sull'intolleranza – inclusa l'intolleranza espressa dal nazionalismo aggressivo e dall'etnocentrismo –, sulla discriminazione e sull'ostilità verso i minori, i migranti e le persone di origine straniera".

Ancora, si consideri la ***Raccomandazione di politica generale n. 15*** della **Commissione contro il razzismo e l'intolleranza del Consiglio d'Europa (ECRI), del 21 marzo 2016**.

In essa si specifica che ai fini della raccomandazione si intende per **discorso dell'odio** «il fatto di fomentare, promuovere o incoraggiare, sotto qualsiasi forma, la denigrazione, l'odio o la diffamazione nei confronti di una persona o di un gruppo, nonché il fatto di sottoporre a soprusi, insulti, stereotipi negativi, stigmatizzazione o minacce una persona o un gruppo e la giustificazione di tutte queste forme o espressioni di odio testé citate, sulla base della "razza", del colore della pelle, dell'ascendenza, dell'origine nazionale o etnica, dell'età, dell'handicap, della lingua, della religione o delle convinzioni, del **sesso**, del genere, dell'identità di genere, dell'orientamento sessuale e di altre caratteristiche o stato personale».

Infine, nel **2020** in Consiglio d'Europa ha istituito un ***Comitato di Esperti sulla lotta all'incitamento all'odio***, denominato ADI/MSI-DIS, finalizzato a preparare una bozza di raccomandazione per affrontare e regolamentare il discorso dell'odio nell'ambito del quadro dei diritti umani.

Interessantissima è la ***Recommendation of the Committee of Ministers to member States on combating hate speech***, emanata nel **maggio 2022** dal ***Comitato di esperti sulla lotta all'incitamento all'odio*** istituito nel 2020, che costituisce oggi un documento di fondamentale importanza in quanto propone una strategia complessiva per prevenire e combattere i discorsi d'odio, anche con riferimento alla dimensione virtuale.

Con questa raccomandazione il Comitato ha chiesto ai governi dei Paesi membri di impegnarsi nell'elaborazione di strategie volte a prevenire e combattere l'*hate speech*, facendo leva sull'adozione di un quadro giuridico adeguato e compatibile con il principio del *balancing of interests* tra diritto al rispetto della vita privata, diritto alla libertà di espressione e divieto di discriminazione.

Particolare attenzione è dedicata all'incitamento all'odio online. A questo proposito, il Comitato ha chiesto agli Stati di definire e delineare i doveri e le responsabilità degli attori statali e non statali nell'affrontare questa piaga. Gli Stati membri dovrebbero inoltre creare regole e procedure chiare per una cooperazione efficace con e tra tali attori per quanto riguarda la valutazione e l'indagine sull'incitamento all'odio *online*. In relazione ai fornitori di servizi Internet, il Comitato invita gli Stati a richiedere a coloro che operano all'interno della loro giurisdizione il rispetto dei diritti umani, ad applicare il principio di *due diligence* in tutte le loro operazioni e politiche e, infine, ad adottare misure conformi ai quadri normativi e alle procedure esistenti per contrastare l'incitamento all'odio sulle loro piattaforme.

Indicazioni specifiche sul tema della comunicazione sessista si ritrovano oggi anche nella già richiamata **Convenzione di Istanbul** che, all'**art. 17**, impone agli Stati contraenti la definizione di linee guida rivolte al settore dei media volte a prevenire la violenza contro le donne e rafforzare il rispetto della loro dignità.

**Articolo 17 – Partecipazione del settore privato e dei mass media**

1 Le Parti incoraggiano il settore privato, il settore delle tecnologie dell'informazione e della comunicazione e i *mass media*, nel rispetto della loro indipendenza e libertà di espressione, a partecipare all'elaborazione e all'attuazione di politiche e alla definizione di linee guida e di norme di autoregolazione per prevenire la violenza contro le donne e rafforzare il rispetto della loro dignità.

2 Le Parti sviluppano e promuovono, in collaborazione con i soggetti del settore privato, la capacità dei bambini, dei genitori e degli insegnanti di affrontare un contesto dell'informazione e della comunicazione che permette l'accesso a contenuti degradanti potenzialmente nocivi a carattere sessuale o violento.

- Sul piano dell'**Unione europea**, l'attenzione dedicata al contrasto alla diffusione dell'odio in rete si pone in linea con l'esigenza di tutelare la dignità umana e l'uguaglianza tra cittadini, sancita **all'art. 21, par. 1, della Carta di Nizza**, che vieta qualsiasi forma di discriminazione.

- Nel **2016** la Commissione europea ha varato, insieme a *Facebook*, *Twitter*, *YouTube* ed altre grandi imprese di internet – hanno aderito in seguito *Instagram*, *Google+*, *Snapchat*, *Dailymotion* e *Jeuxvideo.com* – un **Codice di condotta** (*soft law*), che prevede una serie di impegni per combattere la diffusione del linguaggio dell'odio su internet. Nel **2020** ha aderito al codice di condotta anche *Tik Tok*.

Il Codice non sembra limitarsi ad una mera dichiarazione di intenti, ma prevede regole specifiche imponendo alle aziende di introdurre “procedure chiare ed efficaci per esaminare le segnalazioni riguardanti forme illegali di incitamento all’odio nei servizi da loro offerti, in modo da poter rimuovere tali contenuti o disabilitarne l’accesso”.

- Tra gli strumenti di *soft law* la Commissione europea ha adottato anche la **Raccomandazione 2018/334 sulle misure per contrastare i contenuti illegali *online***, volta al promovimento dell'adozione di *standard* minimi nella prevenzione e rimozione degli stessi.
- Stando al documento **UN'UNIONE DELL'UGUAGLIANZA: LA STRATEGIA PER LA PARITÀ DI GENERE 2020-2025**, adottato il **5 marzo 2020**, la violenza *online* contro le donne, ormai dilagante, ostacola anche la partecipazione delle donne alla vita pubblica. Il bullismo, le molestie e le ingiurie sui *social media* hanno effetti di ampia portata sulla vita quotidiana delle donne e delle ragazze.

L’Unione europea era già intervenuta con strumenti vincolanti, adottando la **decisione quadro 2008/913/GAI sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale**, nella quale, tra i reati a stampo razzista o xenofobo, è stata prevista «l’istigazione pubblica alla violenza o all’odio nei confronti di un gruppo di persone, o di un suo membro, definito in riferimento alla razza, al colore, alla religione, all’ascendenza all’origine nazionale o etnica».

Altro strumento importante è la **Direttiva 2012/29/UE sui diritti delle vittime di reato** che mira, tra l'altro, a garantire giustizia, protezione e sostegno alle vittime di reati basati sull'odio e sull'incitamento all'odio.
Essa impone agli Stati membri di garantire che le vittime di reato siano trattate in modo equo e non discriminatorio, accordando particolare attenzione alle vittime di reati motivati da pregiudizi o discriminazioni.

**IN PROSPETTIVA….**

- Più attenta attuazione del *Codice di condotta;*

- Adozione di una modifica **dell'art. 83, par. 1), del Trattato sul Funzionamento dell'Unione Europea (TFUE):** Parlamento e Consiglio potrebbero deliberare, con direttiva, norme minime sulla definizione dei reati e delle sanzioni; verrebbero ivi inclusi (fra i reati dell'UE) i crimini d'odio e l'incitamento all'odio, anche di stampo sessista.

- Pronta approvazione della **PROPOSTA DI DIRETTIVA sul contrasto alla violenza contro le donne e la violenza domestica**.

# CONSIDERAZIONI CONCLUSIVE

- **Quali obblighi incombono dunque oggi in capo agli Stati in relazione alla violenza di genere *online* o facilitata dalle tecnologie?**
- Innanzitutto, gli Stati hanno l'obbligo in materia di diritti umani di garantire che sia gli agenti statali che quelli non statali si **astengano** dal porre in essere qualsiasi atto di discriminazione o violenza contro le donne.
- Gli Stati hanno la **responsabilità diretta riguardo alla violenza perpetrata da agenti dello Stato stesso**. Essi anche hanno **obblighi di dovuta diligenza** per **prevenire, indagare e punire atti di violenza contro le donne** commessi da società private, come intermediari di Internet
- La circostanza che le violazioni siano perpetrate oltre i limiti territoriali e giurisdizionali degli Stati rende difficile anche per le autorità, comprese le forze dell'ordine, identificare, indagare, perseguire i colpevoli e fornire rimedi ai sopravvissuti alla violenza di genere. A tal fine la **cooperazione tra gli Stati assume un ruolo cruciale**.

**Prevenzione**

La prevenzione comprende misure volte a sensibilizzare l'opinione pubblica sulla violenza contro le donne e le ragazze facilitata dalle *ICTs*, nonché per trovare e fornire informazioni sui servizi e sulle tutele legali disponibili per fermare le violazioni e per prevenire il loro ripetersi.

**Protezione**

L'obbligo di tutelare le vittime della violenza *online* contro le donne comprende l'istituzione di procedure per la rimozione immediata di contenuti dannosi basati sul genere attraverso l'eliminazione del materiale originale o la cessazione della sua distribuzione. Anche la protezione richiede un'azione giudiziaria immediata sotto forma di ordinanze dei tribunali nazionali e un intervento tempestivo degli intermediari Internet e, occasionalmente, potrebbe essere richiesta anche una cooperazione extraterritoriale tra Stati. L'obbligo di protezione comprende anche la fornitura di servizi accessibili per i sopravvissuti, come ad esempio servizi di assistenza legale.

**Obbligo di perseguire penalmente**

L'azione penale consiste nell'avvio di un procedimento contro i presunti autori. Le forze dell'ordine spesso banalizzano la violenza *online* contro le donne e, non di rado, le loro reazioni sono purtroppo caratterizzate da un atteggiamento di 'colpevolizzazione' della vittima quando si occupano di questi casi. Il risultato di questo atteggiamento è una cultura del silenzio e della sottovalutazione del rischio e del danno, con le donne vittime riluttanti a parlare apertamente per paura di essere colpevolizzate.

Anche quando le vittime riescono a denunciare un caso e a far avviare un'indagine, esse spesso incontrano ulteriori ostacoli dati dalla mancanza di conoscenze e capacità tecniche nel settore giudiziario. Inoltre, a volte i costi del contenzioso impediscono a molte donne, in particolare a quelle più povere, di portare avanti delle azioni giudiziarie.

**Obbligo di punire**

Esso comporta il dovere di punire gli autori dei loro crimini mediante sanzioni necessarie e proporzionate al reato. La certezza di un'adeguata punizione trasmette il messaggio che la violenza facilitata dalle ICT contro le donne e le ragazze non sarà tollerata, il che è particolarmente importante per le donne vittime di violenza *online*, che spesso non ricevono una risposta efficace dalle autorità statali e percepiscono l'esistenza di una cultura di impunità per gli autori del reato.

**Risarcimento, riparazione e rimedi**

Nella maggior parte dei casi, alle vittime della violenza di genere vengono concessi risarcimenti civili che includono una compensazione finanziaria per coprire i costi delle perdite quantificabili subite (come spese per cure mediche, perdita di salario e danni materiali), infortuni e perdite non quantificabili. Le misure di riparazione comprendono anche l'immediata rimozione dei contenuti lesivi nonché forme di restituzione, riabilitazione, soddisfazione e garanzie di non ripetizione, combinando misure simboliche, materiali, individuali, e collettive, a seconda delle circostanze e delle pretese avanzate dalla vittima. Tali mezzi dovrebbero includere anche un'ingiunzione immediata per impedire la pubblicazione di contenuti dannosi.

Emerge, in conclusione, come la questione della violenza contro le donne *online* e/o facilitata dalle *ICTs* stia diventando sempre più **rilevante nell'agenda internazionale ed europea**: gli sviluppi riscontrati si dispiegano tra la disciplina volta a promuovere misure di tipo preventivo e di sensibilizzazione culturale verso questa piaga e quella che mira da un lato a promuovere la parità di genere e dall'altro a contrastare la violenza contro le donne.

Nella **Raccomandazione generale n. 35 (2017)**, il Comitato EDAW aveva raccomandato agli Stati di incoraggiare il settore privato, comprese le imprese e le società transnazionali, ad adottare tutte le misure appropriate per eliminare ogni forma di discriminazione, compresa la violenza contro le donne, e ad assumersi la responsabilità per ogni forma di violenza ad esse riferibile. Ne consegue che i siti *web* e i *social media* dovrebbero essere incoraggiati a creare o rafforzare meccanismi incentrati sull'eliminazione degli stereotipi di genere e a porre fine a qualsiasi violenza di genere commessa sulle loro piattaforme.
Purtroppo, però, la realtà ci impone di evidenziare come nonostante gli sforzi in atto, spesso le **politiche e le leggi attuali a tutti i livelli non siano ancora riuscite ad affrontare ed eradicare questo problema in modo adeguato.**

## Quali le strategie per promuovere l'eguaglianza di genere nell'accesso alle tecnologie e nella partecipazione *online*?

L'UE dovrebbe continuare ad affrontare il problema delle barriere strutturali alla base del divario digitale di genere e sostenere una trasformazione digitale inclusiva ed equa. Ciò significa anche promuovere un **approccio partecipativo**, che tenga conto della dimensione di genere, nelle politiche, nei progetti e nei programmi di sviluppo che sostengono la trasformazione digitale dei paesi partner.

L'azione dell'UE dovrebbe contribuire a:

- promuovere **riforme politiche e normative** nei paesi partner, garantendo che la trasformazione digitale sia coerente con l'approccio antropocentrico dell'UE, apportando benefici a tutti, tutelando al contempo i diritti umani, sia *online* che *offline*, e garantendo un ciberspazio sicuro dove i dati siano protetti in linea con le norme dell'UE (ad esempio il Regolamento generale sulla protezione dei dati del 2016);

- migliorare l’accesso delle ragazze e delle donne a una **connettività digitale sicura e accessibile**, raggiungendo le aree rurali e remote;
- **promuovere l’alfabetizzazione digitale** per le ragazze durante la scuola, nonché le competenze digitali per l’occupazione e l’imprenditorialità, affrontando al contempo il problema dei ruoli e degli stereotipi di genere che allontanano le donne e le ragazze dalla tecnologia;
- sostenere le donne innovatrici e imprenditrici nel settore digitale in molteplici ecosistemi industriali, per costruire un'economia digitale inclusiva ad esempio attraverso partenariati pubblico-privato quali la Società finanziaria internazionale, con l’obiettivo di colmare il divario digitale di genere nelle grandi aziende tecnologiche;
- sostenere la prestazione di servizi pubblici e privati attraverso canali, tecnologie e servizi digitali che tengano conto della dimensione di genere (ad esempio *e-government*, servizi finanziari digitali) e che rafforzeranno **l'inclusione e la partecipazione delle donne e delle ragazze alla società.**


GRAZIE PER LA VOSTRA ATTENZIONE!!

claudia.morini@unisalento.it