

---

**XIX LEGISLATURA**

---

Doc. **XXIII**  
n. **18**

**COMMISSIONE PARLAMENTARE DI INCHIESTA  
SUL FEMMINICIDIO, NONCHÉ SU OGNI FORMA DI  
VIOLENZA DI GENERE**

*(istituita con legge 9 febbraio 2023, n. 12)*

(composta dai deputati: *Semenzato, Presidente, Almici, Ascari, Bonetti, Caretta, Dalla Chiesa, Ferrari, Forattini, Gebhard, Ghio, Lancellotta, Loizzo, Morfino, Patriarca, Pulciani, Ravetto, Segretario, Zanella, Segretario, Zurzolo*, e dai senatori: *Ancorotti, Biancofiore, Bilotti, Campione, Cosenza, Cucchi, D'Elia, Vicepresidente, Fallucchi, Leonardi, Vicepresidente, Maiorino, Minasi, Sbrollini, Sensi, Ternullo, Testor, Tosato, Unterberger, Valente*)

**RELAZIONE SULLA DIMENSIONE DIGITALE  
DELLA VIOLENZA CONTRO LE DONNE**

**(ai sensi dell'articolo 2, comma 1, lettere a) e b), della legge 9 febbraio 2023, n. 12)**

(Relatori: **on. SEMENZATO, sen. LEONARDI, sen. D'ELIA**)

*Approvata dalla Commissione nella seduta del 22 aprile 2026*

---

*Comunicata alle Presidenze il 22 aprile 2026  
ai sensi dell'articolo 1, comma 2, della legge 9 febbraio 2023, n. 12*

---

PAGINA BIANCA



*Senato della Repubblica - Camera dei Deputati*

COMMISSIONE PARLAMENTARE DI INCHIESTA SUL FEMMINICIDIO,  
NONCHÈ SU OGNI FORMA DI VIOLENZA DI GENERE

Signor Presidente,

desidero informarLa che la Commissione, che ho l'onore di presiedere, nella seduta odierna ha approvato all'unanimità la Relazione sulla Dimensione digitale della violenza contro le donne, ai sensi dell'articolo 2, comma 1, lettere *a)* e *b)*, della legge 9 febbraio 2023, n. 12 (Doc. XXIII, n. 18).

L'occasione mi è gradita per rinnovarLe i sensi della mia più alta considerazione.

Martina Semenzato

A handwritten signature in blue ink that reads "Martina Semenzato".

---

On. Lorenzo FONTANA  
Presidente della Camera dei deputati

*Senato della Repubblica - Camera dei Deputati*

COMMISSIONE PARLAMENTARE DI INCHIESTA SUL FEMMINICIDIO,  
NONCHÉ SU OGNI FORMA DI VIOLENZA DI GENERE

Signor Presidente,

desidero informarLa che la Commissione, che ho l'onore di presiedere, nella seduta odierna ha approvato all'unanimità la Relazione sulla Dimensione digitale della violenza contro le donne, ai sensi dell'articolo 2, comma 1, lettere *a)* e *b)*, della legge 9 febbraio 2023, n. 12 (Doc. XXIII, n. 18).

L'occasione mi è gradita per rinnovarLe i sensi della mia più alta considerazione.

Martina Semenzato

---

Sen. Ignazio LA RUSSA  
Presidente del Senato della Repubblica

## INDICE

|                                                                                                                     |    |
|---------------------------------------------------------------------------------------------------------------------|----|
| PREMESSA .....                                                                                                      | 6  |
| 1. Obiettivi dell'inchiesta, soggetti auditi e tematiche da approfondire .                                          | 9  |
| 2. La natura, la portata e le conseguenze della dimensione digitale della violenza contro le donne .....            | 13 |
| 3. I principali tipi di violenza <i>on line</i> .....                                                               | 14 |
| 3.1. Il linguaggio d'odio in rete (la misoginia) .....                                                              | 16 |
| 3.1.1. Le « palestre » di misoginia: gli « <i>AI companion</i> » o <i>app</i> di compagnia .....                    | 19 |
| 4. Le conseguenze della dimensione digitale della violenza contro le donne .....                                    | 21 |
| 5. La dimensione digitale della violenza contro le donne e la valutazione del rischio nel rapporto del GREVIO ..... | 21 |
| 5.1. La Raccomandazione generale n. 1 sulla dimensione digitale della violenza contro le donne .....                | 22 |
| 6. Le principali forme di violenza digitale .....                                                                   | 24 |
| 6.1. Condivisione non consensuale di immagini intime .....                                                          | 24 |
| 6.2. Molestie sessuali .....                                                                                        | 24 |
| 6.3. <i>Cyberstalking</i> .....                                                                                     | 25 |
| 6.4. La violenza psicologica <i>on line</i> .....                                                                   | 26 |
| 6.5. L'abuso economico .....                                                                                        | 26 |
| 6.6. Il <i>child grooming</i> .....                                                                                 | 27 |
| 6.7. L' <i>orbiting</i> .....                                                                                       | 28 |
| 6.8. Il <i>ghosting</i> .....                                                                                       | 29 |
| 6.9. Il <i>sexting</i> .....                                                                                        | 29 |
| 6.10. Le ulteriori forme .....                                                                                      | 30 |
| Parte I – LA TUTELA CIVILISTICA DELLE IMMAGINI DELLE PERSONE .....                                                  | 33 |
| 1. La tutela civile .....                                                                                           | 33 |
| 1.1. Il fondamento normativo .....                                                                                  | 33 |
| 1.2. La rilevanza costituzionale .....                                                                              | 34 |
| 1.3. Le indicazioni sovranazionali .....                                                                            | 34 |
| 2. Il risarcimento del danno conseguente all'abuso dell'immagine altrui .....                                       | 36 |
| 2.1. L'accertamento della effettività della lesione .....                                                           | 37 |
| 2.2. Il criterio risarcitorio del c.d. prezzo del consenso .....                                                    | 37 |

|                                                                                                                                               |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------|----|
| Parte II – LA TUTELA PENALE: LE IPOTESI DI REATO .....                                                                                        | 40 |
| 1. Diffusione non consensuale di immagini sessualmente esplicite .....                                                                        | 40 |
| 1.1. L'origine .....                                                                                                                          | 40 |
| 1.2. Gli elementi costitutivi .....                                                                                                           | 41 |
| 1.3. La nozione di « contenuti sessualmente espliciti » .....                                                                                 | 43 |
| 1.4. Il consenso a farsi riprendere non esclude il reato .....                                                                                | 44 |
| 1.4.1. I contenuti su « <i>OnlyFans</i> » .....                                                                                               | 45 |
| 1.5. Il rapporto con il reato di <i>stalking</i> .....                                                                                        | 46 |
| 1.6. Le criticità dei c.d. <i>shame crimes</i> .....                                                                                          | 46 |
| 1.6.1. I c.d. superdiffusori .....                                                                                                            | 47 |
| 1.6.2. I rimedi .....                                                                                                                         | 48 |
| 2. Il delitto di diffusione di riprese e registrazioni fraudolente .....                                                                      | 50 |
| 2.1. Gli elementi costitutivi .....                                                                                                           | 50 |
| 2.2. I rapporti con il c.d. <i>revenge porn</i> .....                                                                                         | 52 |
| 2.3. L'elemento soggettivo .....                                                                                                              | 52 |
| 2.4. Le telecamere di videosorveglianza interne alle abitazioni .....                                                                         | 53 |
| 2.4.1. Gli accorgimenti .....                                                                                                                 | 53 |
| 3. Il delitto di illecita diffusione di contenuti generati o manipolati con sistemi di intelligenza artificiale .....                         | 53 |
| 3.1. Gli elementi costitutivi .....                                                                                                           | 53 |
| 3.2. « Non con la mia faccia. #IoDenuncio » .....                                                                                             | 56 |
| 4. Il trattamento illecito di dati personali .....                                                                                            | 57 |
| 4.1. I dati personali .....                                                                                                                   | 57 |
| 4.2. Gli elementi costitutivi del reato .....                                                                                                 | 57 |
| 4.2.1. Il bene giuridico tutelato .....                                                                                                       | 58 |
| 4.2.2. Il nocumento .....                                                                                                                     | 58 |
| 4.2.3. La pubblicazione di una foto altrui sui <i>social</i> .....                                                                            | 59 |
| 4.3. La diffusione del numero di telefono di una persona mediante il suo inserimento in una <i>chat</i> a contenuto erotico .....             | 59 |
| 4.4. La diffusione su siti porno di fotomontaggi utilizzando foto prelevate da <i>Facebook</i> .....                                          | 59 |
| 5. La sostituzione di persona .....                                                                                                           | 59 |
| 5.1. Gli elementi costitutivi .....                                                                                                           | 59 |
| 5.2. Il concorso con il delitto di trattamento illecito di dati personali .....                                                               | 60 |
| 6. La diffamazione .....                                                                                                                      | 61 |
| 6.1. Gli elementi costitutivi .....                                                                                                           | 61 |
| 6.2. La presenza virtuale .....                                                                                                               | 61 |
| 6.3. La diffusione di un messaggio diffamatorio attraverso l'uso di un <i>social network</i> (come <i>Instagram</i> o <i>Facebook</i> ) ..... | 62 |
| 6.4. Il rapporto con il reato di <i>stalking</i> ... ..                                                                                       | 62 |
| 6.4.1. ... e di trattamento illecito di dati personali .....                                                                                  | 63 |

|                                                                                                                                          |    |
|------------------------------------------------------------------------------------------------------------------------------------------|----|
| 7. La truffa .....                                                                                                                       | 63 |
| 7.1. Gli elementi costitutivi .....                                                                                                      | 63 |
| 7.2. La truffa telematica .....                                                                                                          | 63 |
| 7.3. Il rapporto con il reato di illecito trattamento dei dati personali .....                                                           | 64 |
| 8. La violenza sessuale virtuale .....                                                                                                   | 64 |
| 8.1. Gli elementi costitutivi .....                                                                                                      | 64 |
| 9. Il <i>cyberstalking</i> .....                                                                                                         | 66 |
| 9.1. Gli elementi costitutivi .....                                                                                                      | 66 |
| 10. La istigazione al suicidio .....                                                                                                     | 67 |
| 10.1. Gli elementi costitutivi .....                                                                                                     | 67 |
| 11. L'estorsione sessuale ( <i>sextortion</i> ) .....                                                                                    | 68 |
| 11.1. Gli elementi costitutivi .....                                                                                                     | 68 |
| 11.2. L'uso di <i>deepnude</i> .....                                                                                                     | 69 |
| 12. Le lacune .....                                                                                                                      | 70 |
| Parte III – CONSEGUENZE A LIVELLO PSICOLOGICO .....                                                                                      | 71 |
| 1. Il trauma .....                                                                                                                       | 71 |
| 1.1. La violenza simbolica .....                                                                                                         | 72 |
| 1.2. Le carenze .....                                                                                                                    | 72 |
| 1.3. Le azioni concrete proposte dal Consiglio nazionale dell'ordine degli psicologi (CNOP) nella prevenzione della violenza digitale .. | 72 |
| Parte IV – LA TUTELA OFFERTA DALLE PIATTAFORME .....                                                                                     | 75 |
| 1. Le segnalazioni .....                                                                                                                 | 75 |
| 1.1. Le criticità .....                                                                                                                  | 75 |
| 1.2. I rimedi .....                                                                                                                      | 76 |
| 1.2.1. I modelli di visione e di linguaggio e gli algoritmi .....                                                                        | 78 |
| 1.2.2. I « <i>trusted flaggers</i> » (i segnalatori attendibili) .....                                                                   | 79 |
| 1.3. L'esperienza « Meta » .....                                                                                                         | 80 |
| 1.4. L'attuazione della Direttiva <i>E-evidence</i> .....                                                                                | 81 |
| 2. L'anonimato <i>on line</i> .....                                                                                                      | 82 |
| 2.1. La celere identificazione del responsabile .....                                                                                    | 82 |
| 3. La rimozione immediata dei contenuti .....                                                                                            | 83 |
| 3.1. La crittografia .....                                                                                                               | 83 |
| 4. La scansione delle immagini .....                                                                                                     | 83 |
| 4.1. La pseudonimizzazione tramite il codice <i>hash</i> .....                                                                           | 83 |
| 4.2. Gli ulteriori rimedi .....                                                                                                          | 85 |
| Parte V – LA POLIZIA POSTALE E DELLE COMUNICAZIONI .....                                                                                 | 87 |
| 1. La sicurezza informatica .....                                                                                                        | 87 |
| 1.1. Il dato normativo .....                                                                                                             | 87 |
| 1.2. I compiti .....                                                                                                                     | 87 |

|                                                                                                                       |     |
|-----------------------------------------------------------------------------------------------------------------------|-----|
| Parte VI – LA PROTEZIONE OFFERTA DALLE <i>AUTHORITY</i> .....                                                         | 92  |
| 1. L'Autorità per le garanzie nelle comunicazioni (AGCOM) .....                                                       | 92  |
| 1.1. La natura e le funzioni .....                                                                                    | 92  |
| 1.2. I poteri sulle piattaforme .....                                                                                 | 92  |
| 1.3. Il gruppo <i>Facebook</i> « Mia moglie » .....                                                                   | 94  |
| 1.4. La piattaforma « <i>Phica.eu</i> » .....                                                                         | 96  |
| 1.5. Le criticità e i rimedi .....                                                                                    | 98  |
| 2. Il Garante per la protezione dei dati personali .....                                                              | 99  |
| 2.1. La natura e le funzioni .....                                                                                    | 99  |
| 2.2. Il reclamo al Garante .....                                                                                      | 100 |
| 2.3. Le segnalazioni .....                                                                                            | 103 |
| 2.3.1. Il <i>revenge porn</i> .....                                                                                   | 103 |
| 2.3.2. Il regolamento del Garante n. 1 del 2019 .....                                                                 | 104 |
| 2.4. <i>Deepfake</i> : la scheda informativa sui rischi dell'uso malevolo di questa nuova tecnologia .....            | 104 |
| 2.4.1. <i>Deepnude</i> : il provvedimento n. 789 del 18 dicembre 2025 .                                               | 111 |
| 2.5. I limiti di tutela .....                                                                                         | 113 |
| 3. L'Agenzia per la Cybersicurezza Nazionale (ACN) .....                                                              | 114 |
| 3.1. La natura e le funzioni .....                                                                                    | 114 |
| 3.2. La consapevolezza del rischio digitale .....                                                                     | 115 |
| 3.2.1. Le tecnologie <i>disruptive</i> .....                                                                          | 116 |
| Parte VII – LE TUTELE PROCESSUALI .....                                                                               | 118 |
| 1. Il processo civile .....                                                                                           | 118 |
| 1.1. La tutela cautelare d'urgenza .....                                                                              | 118 |
| 1.2. Il risarcimento del danno .....                                                                                  | 119 |
| 1.3. La c.d. <i>class action</i> .....                                                                                | 120 |
| Parte VIII – L'EDUCAZIONE DIGITALE .....                                                                              | 122 |
| 1. La formazione in ambito digitale .....                                                                             | 122 |
| 1.1. I minori .....                                                                                                   | 122 |
| 2. I percorsi di alfabetizzazione digitale .....                                                                      | 122 |
| 3. La « <i>media education</i> » .....                                                                                | 122 |
| Parte IX – LE CONCLUSIONI E GLI OBIETTIVI .....                                                                       | 124 |
| 1. Le conclusioni .....                                                                                               | 124 |
| 2. Gli obiettivi .....                                                                                                | 127 |
| PUNTO 1 – CONTRASTO ALL'ANONIMATO <i>ON LINE</i> : IDENTIFICAZIONE DELL'UTENTE .....                                  | 128 |
| PUNTO 2 – OBBLIGO DEI GESTORI DELLE PIATTAFORME DI MONITORAGGIO, INTERVENTO TEMPESTIVO E CONSERVAZIONE DEI DATI ..... | 128 |

|                                                                                                                                                                  |     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| PUNTO 3 – COMUNICAZIONE DA PARTE DEI GESTORI DELLE PIATTAFORME DELLE <i>POLICY</i> E DELLE MODALITÀ DI SEGNA- LAZIONE .....                                      | 128 |
| PUNTO 4 – ESTENSIONE A TUTTE LE PIATTAFORME DELL'OB- BLIGO DELLA REGISTRAZIONE DEL CODICE « <i>HASH</i> » .....                                                  | 128 |
| PUNTO 5 – « <i>DASPO</i> » DIGITALE .....                                                                                                                        | 129 |
| PUNTO 6 – ESTENSIONE DEL MECCANISMO DI SEGNALAZIONE AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI .....                                                        | 129 |
| PUNTO 7 – MAGGIORI POTERI DI « <i>ENFORCEMENT</i> » DELL'AUTO- RITÀ PER LE GARANZIE NELLE COMUNICAZIONI (AGCOM) .....                                            | 129 |
| PUNTO 8 – ACCELERAZIONE DELLE PROCEDURE PER IL RILA- SCIO DELLA QUALIFICA DI SEGNALATORE ATTENDIBILE .....                                                       | 129 |
| PUNTO 9 – POTENZIAMENTO DELLA SICUREZZA DEI MINORI ...                                                                                                           | 130 |
| PUNTO 10 – POTENZIAMENTO DELLE COMPETENZE TECNICO- INVESTIGATIVE NEL CONTRASTO ALLA VIOLENZA DIGITALE .                                                          | 130 |
| PUNTO 11 – POTENZIAMENTO DEL TRATTAMENTO SANZIONA- TORIO PER LA C.D. <i>SEXTORTION</i> .....                                                                     | 130 |
| PUNTO 12 – INTRODUZIONE DEL REATO DI DIFFUSIONE ILLE- CITA DI CONTENUTI SESSUALMENTE ESPlicitI GENERATI O ALTERATI CON SISTEMI DI INTELLIGENZA ARTIFICIALE ..... | 130 |
| PUNTO 13 – PRESCRIZIONE DEL DIVIETO DI ACCESSO A INTER- NET PER I SOTTOPOSTI AGLI ARRESTI DOMICILIARI PER REATI DIGITALI .....                                   | 130 |
| PUNTO 14 – PATROCINIO A SPESE DELLO STATO PER I « <i>GENDER- BASED DIGITAL CRIMES</i> » .....                                                                    | 131 |
| PUNTO 15 – DEINDICIZZAZIONE .....                                                                                                                                | 131 |
| PUNTO 16 – RICOGNIZIONE DEGLI ASSETTI NORMATIVI IN MA- TERIA DI PREVENZIONE E CONTRASTO DELLA VIOLENZA DI GENERE DIGITALE .....                                  | 131 |
| PUNTO 17 – INTERVENTO SUL CODICE DEONTOLOGICO DEI GIORNALISTI PER CONTENERE IL FENOMENO DELLA « SUPER- DIFFUSIONE » .....                                        | 131 |
| PUNTO 18 – POTENZIAMENTO DELLA EDUCAZIONE DIGITALE, DELL'USO CONSAPEVOLE DEI MEDIA E DELLA CULTURA DELLA PARITÀ DI GENERE .....                                  | 132 |
| PUNTO 19 – ISTITUZIONE DI UN TAVOLO TECNICO PERMANENTE O OSSERVATORIO CON RACCOLTA DI DATI .....                                                                 | 132 |
| PUNTO 20 – ASSISTENZA LEGALE E PSICOLOGICA E TECNICA .                                                                                                           | 132 |

PREMESSA <sup>(1)</sup>

Con violenza digitale, o cyberviolenza, si intendono tutte quelle forme di violenza attuate mediante tecnologie digitali e in ambienti virtuali quali piattaforme *social*, «*app*» di messaggistica e «*forum on line*».

La violenza *on line* è un fenomeno globale, acuitosi dopo la pandemia di Covid-19, che ostacola la piena realizzazione dell'uguaglianza di genere e viola i diritti delle donne <sup>(2)</sup> tutelati a livello internazionale <sup>(3)</sup>.

Può assumere molte forme: molestie, minacce, *stalking*, condivisione non consensuale di immagini intime, sostituzione di persona, illecita diffusione di contenuti generati o manipolati con sistemi di intelligenza artificiale, fino ad arrivare alla violenza sessuale e all'estorsione <sup>(4)</sup>.

Gli autori possono essere partner o ex partner, colleghi, compagni di scuola o perfetti sconosciuti che si fanno forti della «immunità» assicurata loro dall'«anonimato» in rete.

La presente inchiesta ha consentito di appurare che la violenza di genere *on line* non è un fenomeno marginale e non è neanche circoscritto a casi isolati: è una componente strutturale dell'ecosistema digitale <sup>(5)</sup>.

La violenza di genere contro le donne, perpetrata nella sfera digitale, ha un impatto rilevante sulla loro vita e, segnatamente, sulla salute psicologica e fisica, sul senso di sicurezza e sulla reputazione. Può limitare il diritto delle donne di esprimersi in modo libero e senza paura dissuadendole dalla partecipazione digitale alla vita politica, sociale e culturale. L'abuso odioso a cui le donne sono sottoposte negli ambienti digitali induce molte donne a ritirarsi dalla partecipazione *on line*, dall'esprimere le proprie opinioni sulle piattaforme *on line*. Particolarmente esposte sono coloro che difendono i diritti umani delle donne e delle ragazze, le giornaliste e chi opera nel mondo della

(1) Alla stesura della Relazione ha contribuito, ai sensi dell'articolo 23 del Regolamento interno, il collaboratore esterno dottor Valerio de Gioia, magistrato.

(2) Per l'articolo 3 della Convenzione del Consiglio di Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica, firmata a Istanbul l'11 maggio 2011, ratificata con legge 27 giugno 2013, n. 77, la violenza contro le donne è una violazione dei diritti umani e una forma di discriminazione. La medesima Convenzione stabilisce che lo Stato deve garantire che il diritto delle donne di vivere libere dalla violenza sia preservato, specialmente nella fase delle indagini, innanzitutto attraverso una corretta valutazione e gestione dei rischi di letalità, di gravità della situazione, di reiterazione di comportamenti violenti (articolo 51) e, poi, predisponendo un apparato che dia priorità alla sicurezza delle vittime o delle persone in pericolo (articolo 52).

(3) GREVIO (*Group of Experts on Action against Violence against Women and Domestic Violence*), *General Recommendation No. 1 on the Digital Dimension of Violence Against Women*, adopted on 20 October 2021, Council of Europe, Novembre 2021, pag. 9.

(4) Le forme di violenza digitale sono spesso collegate a pratiche di violenza *off line*: forme di condivisione non consensuale o di creazione di contenuti non consensuali si possono intersecare con molestie che avvengono in ambienti fisici e portare a conseguenze molto più gravi, come forme di abuso sessuale, stupro ed eventualmente femminicidio (così Lucia Bainotti, Assistant Professor in Digital and Visual Media Analysis presso il Dipartimento di Media Studies dell'Università di Amsterdam nel corso della audizione del 17 novembre 2025).

(5) Silvia Semenzin, ricercatrice in sociologia digitale presso l'Università Oberta de Catalunya e membro della ong AI Forensics (audizione del 16 ottobre 2025).

politica<sup>(6)</sup>, ma anche i soggetti attivi sui *social media* e/o a livello pubblico<sup>(7)</sup>.

Secondo *Hadja Lahbib*, Commissaria europea per la parità, la preparazione e la gestione delle crisi<sup>(8)</sup>, gli attacchi *on line* alle donne le inducono « *a ritirarsi dai social, ad abbandonarli, a non partecipare attivamente davanti alle istituzioni* »; la diffusione di immagini di donne, spesso artefatte, sono finalizzate a minare la loro reputazione, umiliarle pubblicamente e spingerle ad abbandonare la scena pubblica.

Osserva la coordinatrice delle campagne di *Amnesty International* Italia, *Tina Marinari* che, a finire nel bersaglio degli aggressori, non sono solo donne note e popolari ma anche quelle non esposte mediaticamente alle quali non è rimasta altra possibilità se non quella di rimuovere o di sospendere il proprio *account*. « *È un odio che zittisce, che toglie la voce e la possibilità di replica di fronte a vere e proprie ondate di violenza verbale, che può sfociare in vere e proprie minacce* »<sup>(9)</sup>. Per la Relatrice Speciale delle Nazioni Unite sulla violenza contro le donne, *Reem Alsalem*, vittime della violenza *on line* sono le donne che non hanno paura di esprimere « *la propria opinione, giornaliste, esponenti del mondo politico, attiviste che difendono i diritti umani* »<sup>(10)</sup>.

Il fenomeno è più diffuso di quanto si creda<sup>(11)</sup>: molte donne non sono consapevoli di esserne o esserne state vittime soprattutto quando

(6) La violenza digitale colpisce, in particolare, le donne che prendono parola nello spazio pubblico: giornaliste, attiviste, rappresentanti istituzionali subiscono attacchi digitali come forma di intimidazione e delegittimazione. Secondo l'*International Media Support*, il 73 per cento delle giornaliste ha subito violenza *on line* durante la carriera e il 20 per cento ha subito aggressioni anche nel mondo fisico connesse a episodi digitali, una giornalista su tre ha pensato di abbandonare la professione e otto su dieci si sono autocensurate dopo aver subito attacchi *on line*. L'UNESCO (*United Nations Educational, Scientific and Cultural Organization*) segnala che il 41 per cento delle giornaliste è stato bersaglio di campagne di disinformazione organizzate spesso con il coinvolgimento di leader politici o di figure istituzionali. Le attiviste non sono meno esposte. L'Osservatorio Vox ci racconta ogni anno come le donne siano il primo bersaglio dell'odio *on line*, con picchi proprio quando il femminicidio diventa tema di dibattito pubblico. In generale, cresce quando l'oggetto del dibattito sono i diritti delle donne. Secondo l'Unione interparlamentare – che ha fatto uno studio non recentissimo, nel 2018, ma molto significativo – il 58 per cento delle deputate europee ha subito forme di violenza *on line*, ricevendo commenti denigratori o a connotazione sessuale, e il 46 per cento ha ricevuto minacce di morte o stupro, spesso da autori anonimi. Queste aggressioni mirano a zittire le voci femminili nello spazio democratico. Difendere la parola pubblica delle donne significa difendere la democrazia stessa (*Barbara Leda Kenny, Senior Gender Expert della Fondazione G. Brodolini*, audizione del 22 ottobre 2025).

(7) Negli ultimi anni abbiamo assistito a una crescita esponenziale della violenza di genere *on line* nelle sue diverse forme. Non è un fenomeno solo italiano, come spiegato da *Silvia Semenzin*, ricercatrice in sociologia digitale presso l'Università Oberta de Catalunya e membro della ong AI Forensics: « *nonostante le leggi, nonostante si parli sempre di più di questa tematica e non manchino gli scandali anche in questo senso, i dati ci dicono che il fenomeno sta crescendo. Per quanto riguarda l'Italia, secondo un report di Amnesty International (il barometro dell'odio del 2024), gli episodi di violenza di genere sono triplicati* » (audizione del 16 ottobre 2025, cit.).

(8) Audizione del 21 novembre 2025.

(9) Audizione del 24 novembre 2025.

(10) Audizione del 20 novembre 2025. Il vero problema, ha fatto notare l'audita, è che la « *violenza, di fatto, inizia on line, ma poi si materializza con conseguenze pratiche off line, dunque con minacce vere e proprie* ».

(11) Secondo gli ultimi dati diffusi dallo *European Institute for Gender Equality* (EIGE), una donna su due ha subito una forma di violenza *on line*. In Italia rimane il problema dei dati, perché la Polizia postale ha offerto una visione di dati tendenzialmente allarmanti, però si tratta di dati che non sono disaggregati rispetto al genere. In altri termini, non abbiamo un sistema di indagine di dati che vada a individuare quali sono i soggetti che subiscono queste violenze di genere rispetto agli altri soggetti. Vi è una ulteriore difficoltà, « *mentre nella vita reale la reazione di un soggetto per l'interruzione*

le loro immagini intime – vere o generate da sistemi di intelligenza artificiale – vengono diffuse in rete a loro insaputa<sup>(12)</sup>.

Gli auditi concordano sul fatto che quella digitale non è una nuova forma di violenza ma semplicemente un nuovo campo in cui si manifesta la violenza degli uomini contro le donne, sfruttando le tecnologie e la nostra quotidianità sempre più connessa<sup>(13)</sup>. Negli anni la definizione di « violenza » ha subito una evoluzione: alla violenza fisica, sessuale e psicologica si è aggiunta quella economica e, solo di recente, quella digitale, riconosciuta anche nella Direttiva 2024/1385/UE del 14 maggio 2024, sulla lotta alla violenza contro le donne e alla violenza domestica<sup>(14)</sup>.

Approfitrando del senso di generale impunità che attraversa le pratiche violente all'interno degli spazi digitali e, traendo forza dall'idea assolutamente errata che l'esercizio della violenza *on line* non abbia lo stesso valore o impatto di quello esercitato negli spazi *off line* e dal mito della tecnologia come soggetto neutrale, la violenza contro le donne *on line* trova oggi nuove forme di espressione e legittimazione.

In questo quadro le piattaforme, le architetture digitali e gli algoritmi alimentano e rinnovano disuguaglianze persistenti, aprendo spazi inediti per la riproduzione, trasformazione e perpetrazione della violenza<sup>(15)</sup>.

La violenza digitale si inserisce in un contesto più ampio di normalizzazione della misoginia e di oggettivazione dei corpi femminili, che trova nelle piattaforme digitali uno spazio di amplificazione e legittimazione. In tale prospettiva, appare necessario che le politiche di contrasto non si limitino a interventi repressivi o regolatori ma includano azioni strutturali di prevenzione culturale, capaci di incidere sui modelli sociali e sui comportamenti.

Accanto dunque alla limitazione dell'impegno e della libertà di espressione delle donne, l'insulto sessualizzato si configura come vera

---

*di una violenza fisica, sessuale, psicologica può essere posta in essere immediatamente, nell'ambito digitale questo non è possibile, perché è uno spazio pubblico nella disponibilità del presunto autore o dell'autore del reato »* (così Rosita Ponticiello, coordinatrice del Dipartimento Pari opportunità dell'Unione Nazionale Camere Civili, audita il 17 novembre 2025).

(12) Internet avrebbe dovuto essere un luogo di incontro, scambio e democratizzazione, per molte donne purtroppo è diventato uno spazio di sorveglianza, di abuso, di ipersessualizzazione, di controllo e di amplificazione dell'odio (così Ivana Bartoletti, vicepresidente e Chief AI Governance and Privacy Officer presso Wipro Technologies e co-fondatrice del Women Leading in AI Network, nell'audizione del 17 novembre 2025).

(13) La violenza digitale « è un'estensione amplificata delle dinamiche di potere e dominio che caratterizzano la violenza di genere. Attraverso parole, immagini, manipolazioni e campagne denigratorie, produce ferite psicologiche e reputazionali profonde, incidendo sulla libertà della persona, sulla dignità e sulla partecipazione civica delle vittime » (così Natalia Re, presidente del MIG-Movimento italiano per la gentilezza, nel corso della audizione del 15 ottobre 2025).

(14) Come rilevato da Barbara Leda Kenny, Senior Gender Expert della Fondazione G. Brodolini, nel corso della audizione del 22 ottobre 2025, la violenza digitale « è complessa e in continua evoluzione, man mano che evolvono gli strumenti tecnologici che utilizziamo. Abbiamo un lessico abbastanza complesso per descriverla, abbiamo parole come cyberstalking, doxing, sextortion, revenge porn, hate speech e molte altre forme ». La sfida – ha sostenuto l'audita – è proprio quella di costruire politiche differenziate che sappiano dare risposta a diverse forme di violenza.

(15) Così Chiara Gius, coordinatrice nazionale del progetto Prin 2022 « rappresentazioni sociali della cyberviolenza contro donne e ragazze » e ricercatrice presso l'Università di Bologna, nel corso della audizione del 20 ottobre 2025.

e propria strategia di esclusione dalla cittadinanza digitale e, in ultima istanza, dalla partecipazione democratica delle donne.

### 1. Obiettivi dell'inchiesta, soggetti auditi e tematiche da approfondire

Il nuovo filone istruttorio è stato deliberato alla luce della scoperta, risalente alla fine del mese di agosto 2025, di siti gravemente sessisti ospitati da piattaforme come *Facebook* e su cui le Procure di Roma, Firenze e Venezia hanno avviato delle indagini sulla base di segnalazioni provenienti, in prima battuta, da aziende private e poi confermate e veicolate dalla Polizia postale.

Si tratta di una materia evidentemente molto delicata sul piano dell'inquadramento penale che chiama in causa la dibattuta questione dell'anonimato in rete che, da strumento di garanzia della libertà di espressione, si può tradurre in uno scudo di impunità per condotte che, al di fuori del mondo virtuale, incorrerebbero in immediatamente severe sanzioni.

Tra l'altro, proprio le modalità con cui i siti sessisti sono stati individuati, mette in evidenza il rapporto sinergico di collaborazione che in questo campo deve intercorrere tra pubblico, in questo caso la Polizia postale e la magistratura, e privato, ad esempio, aziende specializzate sui temi della cybersicurezza.

L'attività di inchiesta è stata sollecitata dalla necessità di verificare se il sistema normativo preveda idonee misure per offrire una tutela piena alle vittime della cosiddetta violenza digitale, così da poter suggerire, in presenza di lacune o criticità, elementi di proposta utili per futuri interventi legislativi, in linea con quanto previsto dall'articolo 2, primo comma, lettera *m*), della legge istitutiva della Commissione (legge 9 febbraio 2023, n. 12).

La presente relazione è il risultato di una ampia attività conoscitiva svolta dalla Commissione, sostanziata in un articolato ciclo di audizioni di rappresentanti di istituzioni e di associazioni, di esperti con competenze diversificate ma anche di vittime di questa nuova forma di violenza, per capire quali sfide dovremo affrontare.

Nello specifico, sono stati auditi:

- *Giuseppe Cascini*, Procuratore Aggiunto presso la Procura della Repubblica di Roma, svolta in modalità segreta (24 settembre 2025);

- *Paolo Reale*, ingegnere esperto di informatica forense (7 ottobre 2025);

- *Francesca Schir*, segretaria del Consiglio nazionale dell'Ordine degli psicologi (CNOP) (7 ottobre 2025);

- *Natalia Re*, Presidente del MIG-Movimento italiano per la gentilezza (15 ottobre 2025);

- *Elisabetta Fersini*, professoressa associata di informatica presso l'Università degli Studi di Milano Bicocca (15 ottobre 2025);

- *Marisa Marraffino*, avvocatessa penalista esperta di diritto dell'informatica, tutela della reputazione aziendale e dei privati nei *new media* e per la gestione della *privacy* (16 ottobre 2025);

- *Silvia Semenzin*, ricercatrice in sociologia digitale presso l'Università Oberta de Catalunya e membro della ong *AI Forensics*, (16 ottobre 2025);
- *Debora Nozza*, professoressa di *Computing Sciences* presso l'Università Bocconi di Milano, specializzata in elaborazione del linguaggio naturale e riconoscimento automatico della misoginia e del linguaggio d'odio *on line* (20 ottobre 2025);
- *Chiara Gius*, coordinatrice nazionale del progetto Prin 2022 « rappresentazioni sociali della cyberviolenza contro donne e ragazze » e ricercatrice presso l'Università di Bologna (20 ottobre 2025);
- *Barbara Leda Kenny*, *Senior Gender Expert* della Fondazione G. Brodolini (22 ottobre 2025);
- *Giacomo Lasorella*, Presidente dell'Autorità Garante per le garanzie nelle comunicazioni (AGCOM) (23 ottobre 2025);
- *Bruno Frattasi*, Direttore dell'Agenzia per la Cybersicurezza Nazionale (ACN) (6 novembre 2025);
- *Rappresentanti della fondazione Pangea Onlus* (10 novembre 2025);
- *Matteo Flora*, presidente dell'associazione PermessoNegato (10 novembre 2025);
- *Cristina Obber*, scrittrice e giornalista (10 novembre 2025);
- *Alex Orłowski*, esperto di *cyberintelligence* (10 novembre 2025);
- *Gino Cecchettin*, presidente della Fondazione Giulia Cecchettin (11 novembre 2025);
- *Jolanda Renga* (13 novembre 2025);
- *Lilia Giugni*, professoressa di Innovazione inclusiva presso l'*University College* di Londra e ricercatrice di Innovazione sociale presso l'Università di Cambridge (17 novembre 2025);
- *Lucia Bainotti*, *Assistant Professor in Digital and Visual Media Analysis* presso il Dipartimento di *Media Studies* dell'Università di Amsterdam (17 novembre 2025);
- *Rappresentanti della Unione Nazionale Camere Civili* (17 novembre 2025);
- *Ivana Bartoletti*, vicepresidente e *Chief AI Governance and Privacy Officer* presso *Wipro Technologies* e co-fondatrice del *Women Leading in AI Network* (17 novembre 2025);
- *Diego Marson*, *Chief Technical Officer* di *Yarix Var Group* (17 novembre 2025);
- *Ivano Gabrielli*, Direttore del Servizio Polizia postale e per la sicurezza cibernetica della Polizia di Stato (17 novembre 2025);
- *Reem Alsalem*, Relatrice Speciale delle Nazioni Unite sulla violenza contro le donne, (audizione del 20 novembre 2025);

- *Rosanna Milone*, responsabile progetti e *Awareness and Advocacy Strategist* della Fondazione Carolina (24 novembre 2025);
- *Rosy Russo*, presidente dell'associazione Parole O\_Stili (24 novembre 2025);
- *Giovanna Mascheroni*, professoressa di sociologia dei processi culturali e comunicativi presso l'Università Cattolica di Milano e coordinatrice di *EU Kids online* Italia (26 novembre 2025);
- *Tina Marinari*, coordinatrice delle campagne di *Amnesty International* Italia (26 novembre 2025);
- *Claudia Trivilino*, *Public Policy Manager* di Meta per Italia e Grecia, e *Laura Bononcini*, *Public Policy Director* di Meta per il Sud-Europa (27 novembre 2025);
- *Florinda Scicolone*, responsabile Pari Opportunità dell'Associazione Italiana Giuristi d'Impresa (AIGI) (27 novembre 2025);
- *Maura Manca*, presidente dell'Osservatorio Nazionale Adolescenza (3 dicembre 2025);
- *Gianna Maria Cappello* e *Maria Ranieri*, presidente e vicepresidente dell'Associazione Italiana per l'Educazione ai *Media* e alla Comunicazione (MED) (4 dicembre 2025);
- *Stefano De Martino*, artista e conduttore televisivo (9 dicembre 2025), *in modalità segreta*;
- *Ernesto Caffo*, presidente della Fondazione S.O.S. Il Telefono Azzurro, e *Giuseppe Magno*, direttore della Fondazione S.O.S. Il Telefono Azzurro e giurista (17 dicembre 2025);
- *Luca Volpe*, avvocato (28 gennaio 2026);
- *Sandra Cioffi*, presidente del Consiglio Nazionale degli Utenti (CNU) (29 gennaio 2026);
- *Barbara Giovanna Bello*, ricercatrice e docente di filosofia del diritto e di giustizia digitale presso l'Università degli Studi della Tuscia (4 febbraio 2026);
- *Mariacristina Sciannamblo*, professoressa associata di sociologia e scienze sociali applicate e coordinatrice del progetto *GIVRE – Gendering Internet. Violence, Resilience and Empowerment in digital spaces* (2023-25) (12 febbraio 2026);
- *Letizia Basile*, presidente dell'associazione di promozione sociale « Iostaccolaspina » (12 febbraio 2026).

Sono state inoltre depositate memorie, a regime libero, da parte dei seguenti soggetti:

- *Paolo Reale*, ingegnere esperto di informatica forense (7 ottobre 2025);
- *Francesca Schir*, Segretaria del Consiglio nazionale dell'ordine degli psicologi (CNOP) (7 ottobre);

- *Natalia Re*, Presidente del MIG-Movimento italiano per la gentilezza (15 ottobre 2025);
- *Marisa Marraffino*, avvocatessa penalista esperta di diritto dell'informatica, tutela della reputazione aziendale e dei privati nei *new media* e per la gestione della *privacy* (16 ottobre 2025);
- *Chiara Gius*, coordinatrice nazionale del progetto Prin 2022 « rappresentazioni sociali della cyberviolenza contro donne e ragazze » e ricercatrice presso l'Università di Bologna (20 ottobre 2025);
- *Barbara Leda Kenny*, *Senior Gender Expert* della Fondazione G. Brodolini (22 ottobre 2025);
- *Giacomo Lasorella*, Presidente dell'Autorità Garante per le garanzie nelle comunicazioni (AGCOM) (23 ottobre 2025);
- *Diego Marson*, *Chief Technical Officer* di Yarix Var Group (17 novembre 2025);
- *Lucia Bainotti*, *Assistant Professor in Digital and Visual Media Analysis* presso il Dipartimento di *Media Studies* dell'Università di Amsterdam, e *Silvia Semenzin*, ricercatrice in sociologia digitale presso l'Università ricercatrice in sociologia digitale presso l'Università Oberta de Catalunya e membro della ong *AI Forensics* (25 novembre 2025);
- *Giovanna Mascheroni*, professoressa di sociologia dei processi culturali e comunicativi presso l'Università Cattolica di Milano e coordinatrice di *EU Kids online Italia* (26 novembre 2025);
- *Maura Manca*, presidente dell'Osservatorio Nazionale Adolescenza (3 dicembre 2025);
- *Ernesto Caffo*, presidente della Fondazione S.O.S. Il Telefono Azzurro (17 dicembre 2025);
- *Save the children Italia* (19 dicembre 2025);
- *Sandra Cioffi*, presidente del Consiglio Nazionale degli Utenti (CNU) (29 gennaio 2026);
- *Marina Terragni*, Autorità Garante per l'Infanzia e l'Adolescenza (9 febbraio 2026);
- *Elisabetta Aldrovandi*, avvocato (2 marzo 2026).

Dalle audizioni sono emerse in particolare le seguenti tematiche che la Commissione ha voluto approfondire sia in relazione a quanto previsto dalla normativa vigente, sia come suggerimento di modifiche e integrazioni alle politiche necessarie:

- 1) anonimato in rete;
- 2) obblighi delle piattaforme;
- 3) semplificazione del meccanismo delle segnalazioni;
- 4) attuazione alle direttive europee;
- 5) poteri della *authority*;
- 6) potenziamento della tutela dei minori;

- 7) disciplina organica dei reati digitali;
- 8) patrocinio a spese dello Stato a prescindere dal reddito anche per i reati digitali;
- 9) regole deontologiche dei giornalisti;
- 10) competenze tecnico-investigative nel contrasto alla violenza digitale;
- 11) tavolo tecnico permanente o osservatorio;
- 12) educazione digitale consapevole.

## **2. La natura, la portata e le conseguenze della dimensione digitale della violenza contro le donne**

Il 17 novembre 2022, all'esito della sua 14<sup>a</sup> riunione, la Piattaforma EDWAV (*Independent Expert Mechanisms on Discrimination and Violence against Women*) organismo che riunisce sette meccanismi indipendenti delle Nazioni Unite e regionali dedicati alla lotta contro la discriminazione e la violenza sulle donne, ha adottato un documento tematico avente ad oggetto «La dimensione digitale della violenza contro le donne secondo i sette meccanismi della Piattaforma EDVAW».

Il documento fornisce una panoramica del problema della violenza contro le donne negli spazi digitali, analizzandone le forme, la portata e le ricadute negative a livello esistenziale e sociale, così da consentire una migliore comprensione del contesto in cui avviene.

Tutte le forme di violenza contro le donne, compresa quella digitale, sono figlie della discriminazione di genere, fondata su nozioni stereotipate di donne e ragazze e sull'idea di una loro inferiorità.

Gli Stati Parte sono obbligati – sulla base dell'articolo 5 della Convenzione ONU sull'eliminazione di tutte le forme di discriminazione contro le donne (*CEDAW, Convention on the Elimination of All Forms of Discrimination Against Women*)<sup>(16)</sup> e degli strumenti regionali applicabili – a combattere tali forme di discriminazione.

La dimensione digitale della violenza contro le donne può includere qualsiasi atto di violenza di genere contro le donne in quanto donne, commesso, facilitato o aggravato, in parte o in tutto, dall'uso delle tecnologie dell'informazione e della comunicazione (TIC), come telefoni cellulari e *smartphone*, internet, piattaforme di *social media* o *email*, dispositivi di tracciamento della geolocalizzazione, droni e intelligenza artificiale (IA)<sup>(17)</sup>.

(16) La norma prevede che gli Stati Parte prendono ogni misura appropriata per modificare i modelli socio-culturali di comportamento degli uomini e delle donne, al fine di conseguire l'eliminazione dei pregiudizi e delle pratiche consuetudinarie o di ogni altro genere che siano basate sull'idea dell'inferiorità o della superiorità dell'uno o dell'altro sesso o su ruoli stereotipati per gli uomini e per le donne.

(17) Per Chiara Gius, coordinatrice nazionale del progetto Prin 2022 «rappresentazioni sociali della cyberviolenza contro donne e ragazze» e ricercatrice presso l'Università di Bologna, dai materiali empirici emerge chiaramente come non si possa parlare di un'unica forma di violenza *on line* contro le donne, ma di un insieme ampio e diversificato di pratiche: dai discorsi d'odio alla condivisione non consensuale di immagini intime, dal *doxing* alla *sextortion*, fino al controllo coercitivo esercitato attraverso *app* di messaggistica, sistemi di geolocalizzazione e dispositivi connessi. Queste pratiche si muovono su piani diversi, cambiano per intenzionalità, attori coinvolti, impatti, ma condividono una comune radice socio-culturale che ne consente

### 3. I principali tipi di violenza *on line*

Presso il Consiglio d'Europa il GREVIO (Gruppo di Esperti sull'Azione contro la Violenza sulle Donne e la Violenza Domestica) indica quattro principali tipi o categorie di violenza *on line* e/o facilitata dalla tecnologia:

1) molestie, violenza o abusi resi possibili da specifiche tecnologie e dispositivi abilitati dalla tecnologia, come la violenza tra partner perpetrata tramite l'uso di *spyware*<sup>(18)</sup> e di altri dispositivi di tracciamento;

2) abusi che avvengono e si amplificano *on line*, come nel caso della condivisione non consensuale di immagini intime (*revenge porn*);

3) forme di abuso generate dalla tecnologia, come la pornografia *deepfake*<sup>(19)</sup> (c.d. *deepnude*<sup>(20)</sup>) e l'abuso dei nostri *avatar*<sup>(21)</sup> nel meta-verso;

4) violenze e abusi sui *social media*.

La violenza contro le donne facilitata dalla tecnologia *on line* comprende un'ampia gamma di comportamenti<sup>(22)</sup>:

1) abuso sessuale basato su contenuti reali (per effetto della creazione, diffusione, distribuzione o condivisione *on line* di fotografie,

---

la diffusione, la persistenza e la normalizzazione. La violenza digitale in altre parole non abita solo gli spazi *on line*, attraversa le relazioni intime, familiari, amicali e professionali, spostandosi costantemente tra dimensioni digitali e materiali e rendendo estremamente difficile tracciare confini netti tra pubblico e privato, tra spazio sociale e spazio tecnologico (audizione del 20 ottobre 2025).

(18) In informatica, uno *spyware* è un tipo di *software* che raccoglie informazioni riguardanti l'attività *on line* di un utente senza il suo consenso. Si tratta, più precisamente, di un *malware* che infetta il *personal computer* o il dispositivo mobile e raccoglie informazioni sull'utente, inclusi i siti che visita, i materiali che scarica, i nomi utente e *password*, le informazioni di pagamento, comprese le *email* inviate e in arrivo.

(19) I *deepfake* sono video in cui un volto viene (senza soluzione di continuità) sostituito da un altro volto, utilizzando algoritmi e apprendimento automatico, con manipolazione del suono così da creare l'illusione che le azioni di un'altra persona siano reali. Come spiegato da Ernesto Caffo, Presidente della Fondazione S.O.S. Il Telefono Azzurro, nel corso della audizione del 17 dicembre 2025, «il tema del deep fake è presente sempre di più nell'ambito della vita di tutti, soprattutto nell'ambito della vita di bambini e adolescenti. Ci sono situazioni in cui le immagini di questi ragazzi vengono associate a dei corpi e di ventano occasioni fortemente di danno per le persone esposte. Abbiamo sempre più vittime dell'alterazione di un'immagine attraverso sistemi di deep fake. L'aumento di immagini pedopornografiche prodotte con l'intelligenza artificiale ha avuto un aumento negli ultimi mesi del 380 per cento, secondo i dati della Internet Watch Foundation».

(20) I *deepnude* sono una sottocategoria di *deepfake*, consistenti in immagini manipolate dalla intelligenza artificiale con lo scopo di rimuovere gli indumenti di una persona, creando immagini finte e sessualmente esplicite. A tale tecnologia si è fatto spesso ricorso per realizzare immagini pornografiche di celebrità e di altre persone, senza il loro consenso, a scopo non solo diffamatorio ma anche estorsivo.

(21) Un *avatar* è una rappresentazione digitale di una persona, un *alter ego* o un'identità virtuale, tipicamente utilizzata nelle comunità *on line* e nei videogiochi; può essere personalizzata per riflettere l'aspetto, la personalità e gli interessi di una persona.

(22) Cfr. *The Digital Dimension of Violence Against Women as addressed by The Seven Mechanisms of the EDVAW Platform Thematic*, cit. pag. 10. Come spiegato da Tina Marinari, coordinatrice delle campagne di Amnesty International Italia, nell'audizione del 24 novembre 2025, Amnesty International intende per «violenza *on line*» qualsiasi atto di violenza *on line*: i commenti misogini e sessisti umilianti; le minacce fisiche e sessuali; gli insulti diretti; la condivisione di immagini intime, video con contenuti sessuali o minacce di farlo; il *doxing* (cioè lo sviluppo e la diffusione non autorizzata di dati personali); l'*outing* forzato, (cioè rivelare l'identità sessuale o di genere di una persona senza il suo consenso); l'*hacking* o anche l'impersonificazione; la sorveglianza digitale (lo *spyware*); gli strumenti di controllo digitale.

video o *clip* audio dal contenuto sessualmente esplicito senza il consenso della vittima) o generati dalla intelligenza artificiale (c.d. *deepnude*)<sup>(23)</sup>;

2) accesso non autorizzato, manipolazione o diffusione di dati personali (c.d. *doxing*)<sup>(24)</sup>;

3) furto d'identità (sostituzione di persona) o creazione di una falsa identità (profilo *fake*);

4) atti che danneggiano la reputazione, l'onore o la credibilità di una persona;

5) atti che implicano controllo, sorveglianza e costante monitoraggio di un soggetto (*stalking on line*)<sup>(25)</sup>;

6) molestie (sessuali) *on line*;

7) cyberbullismo<sup>(26)</sup>;

(23) I *deepnude* – ha sostenuto la Relatrice Speciale delle Nazioni Unite sulla violenza contro le donne Reem Alsalem, nel corso dell'audizione del 20 novembre 2025 – «danneggiano fortemente non solo le donne e le ragazze, ma tutta la società, perché consentono il perpetrarsi della sessualizzazione, oggettificazione e mercificazione del corpo delle donne e delle ragazze, dando l'impressione o, comunque, spingendo la società verso una normalizzazione di comportamenti dannosi, azioni sessualmente dannose nei confronti delle donne e delle ragazze, alimentando l'idea che si possa comperare il sesso, che si possano pagare queste donne per avere sesso in cambio, rendendo accettabile il fatto che si possano avere dei comportamenti degradanti, umilianti e violenti nei confronti delle donne ».

(24) Il *doxing* è l'atto di condividere *on line* le informazioni personali altrui (numero di telefono, indirizzo *email*, indirizzo di casa, contatti professionali) senza consenso dell'interessato, per incoraggiare l'abuso. Come chiarito da Silvia Semenzin, questa pratica «... racconta anche la perversione di una cultura che vuole ottenere quanto più possibile informazioni personali su queste donne e che molto spesso apre ad altre forme di violenza, come lo *stalking*, le molestie e via dicendo » (audizione del 16 ottobre 2025, cit.).

(25) Nei *focus group* e nelle interviste con le operatrici e le attiviste è emersa con forza l'ambivalenza tra il desiderio di proteggere e la tendenza a sorvegliare, soprattutto nelle relazioni intime e familiari. Le tecnologie in questo senso amplificano le dinamiche di controllo. Pensiamo alle *app* di localizzazione usate dai partner o dei genitori, spesso in nome della sicurezza. Gli studi sulla violenza domestica ci dicono come la vulnerabilità sia parte costitutiva di ogni relazione di cura e che il rischio di abuso cresca con l'asimmetria di potere – reale o percepita – che in questa relazione si instaura. La violenza digitale rende queste asimmetrie più visibili, mostrando come le logiche di cura possono trasformarsi in strumenti di controllo. Chiara Gius, nel corso della audizione del 20 ottobre 2025, ha raccontato che «Un dato emblematico riguarda il controllo dei dispositivi tra partner. I dati da noi raccolti ci dicono che se le ragazze lo fanno di nascosto, consapevoli di stare violando spazi non loro, i ragazzi lo fanno apertamente e rivendicando la legittimità di questa loro pretesa, pur mascherandola all'interno di cornici di cura che la rendono più tollerabile ». Secondo una ricerca di Save the Children, per un adolescente su cinque condividere la *password* del telefono è un segno d'amore, il controllo viene mascherato da cura e la violenza viene normalizzata nelle relazioni (come riferisce Barbara Leda Kenny nell'audizione del 22 ottobre 2025). Come rilevato da Simona Lanzoni, vicepresidente della fondazione Pangea Onlus, audita il 10 novembre 2026, molto spesso gli autori di violenza all'interno di una relazione domestica dicono di voler aggiornare il cellulare o, quando si rompe, si offrono di andarne a comprare uno nuovo: in questi nuovi dispositivi, che vengono regalati alla partner, in realtà, sono installate delle *app* «che permettono di geolocalizzarle, di verificare tutte le telefonate, di verificare tutta la messaggistica. Insomma, non sono più libere di avere una vera e propria vita privata ».

(26) Il *cyberbullismo* è il bullismo attuato mediante strumenti e in ambienti digitali. Il *cyberbullismo* è un fenomeno che si è sviluppato a seguito dell'ampio utilizzo dei mezzi di comunicazione *on line* da parte di preadolescenti e adolescenti. La facilità di accesso a personal computer, *smartphone*, *tablet* consente al *cyber-bullo* di commettere atti di violenza fisica e/o psicologica, anche in anonimato, mediante i *social network*, e di

- 8) minacce e violenze sessuali *on line*;
- 9) molestie e abusi dei sé digitali (*avatar*).

### 3.1. Il linguaggio d'odio in rete (la misoginia)

Debora Nozza, professoressa di *Computing Sciences* presso l'Università Bocconi di Milano, specializzata in elaborazione del linguaggio naturale e riconoscimento automatico della misoginia e del linguaggio d'odio *on line*<sup>(27)</sup>, ha rappresentato le problematichità connesse alla individuazione della misoginia<sup>(28)</sup> implicita, a quelle forme di linguaggio *on line* che, pur non usando parole apertamente offensive, trasmettono ostilità, disprezzo e, a volte, vera e propria violenza verso le donne.

Secondo la « Mappa dell'intolleranza » dell'Osservatorio italiano sui diritti, in Italia la metà dei post d'odio *on line* è diretta contro le donne; questa percentuale non è cambiata nel corso degli anni, segno che la misoginia non è un fenomeno episodico ma un problema culturale stabile. Secondo *UN Women*, la misoginia è « *un atteggiamento di disprezzo o avversione verso le donne, che si manifesta attraverso discriminazione, violenza, oggettificazione ed esclusione dalla piena partecipazione sociale e politica* ».

La misoginia esplicita è facilmente riconoscibile dagli algoritmi di intelligenza artificiale a differenza di quella implicita che non usa insulti ma ironia, doppi sensi, stereotipi, componendosi di « un linguaggio offensivo che non usa parole offensive » difficilmente intercettabili dalla IA. Proprio per questo è più pervasiva, più accettata e anche più difficile da individuare.

La ricerca sull'intelligenza artificiale applicata alla misoginia nasce da un'esigenza sociale molto concreta: capire come e dove si formano le radici culturali della violenza di genere. La misoginia *on line* rappresenta un termometro del clima sociale, un segnale precoce di dinamiche che possono evolvere anche in comportamenti violenti<sup>(29)</sup>.

Anche i modelli linguistici più avanzati fanno grande fatica a riconoscere la misoginia implicita, perché bisogna avere conoscenze di contesto, valori sociali, culturali, qualcosa di cui, per il momento,

---

offendere la vittima mediante la diffusione di materiale denigratorio (testi, foto e immagini) o la creazione di gruppi contro. Si tratta di un uso inappropriato della rete, realizzato fuori dal controllo degli adulti, con cui i ragazzi si scambiano contenuti violenti, denigratori, discriminatori, rivolti a coetanei considerati diversi per aspetto fisico, abbigliamento, orientamento sessuale, classe sociale o perché stranieri. Nella fascia di età degli 11enni risultano vittime di cyberbullismo il 17,2 per cento dei maschi e il 21,1 per cento delle femmine; i 13enni coinvolti sono il 12,9 per cento dei ragazzi e il 18,4 per cento delle ragazze; gli adolescenti di 15 anni sono il 9,2 per cento dei maschi e l'11,4 per cento delle femmine (<https://www.salute.gov.it/new/it/tema/salute-del-bambino-e-dell'adolescente/bullismo-e-cyberbullismo/>).

(27) Audizione del 20 ottobre 2025.

(28) Il termine misoginia deriva dal greco antico (*misèō*, « odiare », e *gynè*, « donna ») e indica una forma di pregiudizio di genere che si esprime attraverso comportamenti, atteggiamenti e discorsi discriminatori, ostili o violenti nei confronti delle donne. La misoginia implicita costituisce un'avversione più sottile e nascosta verso le donne, manifestandosi attraverso pregiudizi, stereotipi, discriminazioni o molestie.

(29) L'intelligenza artificiale consente di analizzare milioni di messaggi, *post* e commenti al fine di individuare tendenze, narrazioni ricorrenti, ma soprattutto l'eventuale *escalation*. Questi dati non servono a censurare ma a capire. Permettono di progettare potenzialmente interventi di prevenzione ma anche e soprattutto di educazione digitale, comunicazioni istituzionali più efficaci, basate sui numeri e sulle evidenze.

nessun modello di IA dispone. Ma proprio questi errori sono preziosi perché ci mostrano quanto il pregiudizio sia profondo e anche quanto le tecnologie potenzialmente possano riflettere i limiti del linguaggio umano. Quando un modello non riconosce la misoginia è perché neanche le persone sono in grado di riconoscerla.

I modelli linguistici hanno dei limiti, non sono realmente multiculturali, soprattutto quando lavorano in lingua italiana. Non riconoscono correttamente entità, eventi o metafore, perché la maggior parte della loro conoscenza si forma in lingua inglese o, comunque, sulla base di contesti culturali anglofoni. Questi modelli, inoltre, non « ragionano » davvero ma si basano su informazioni che hanno memorizzato durante l'addestramento.

Con l'attuale ultimo modello di *ChatGPT* si è però registrato un passo avanti: il modello sembra « capire » parti del ragionamento, parti della cultura e delle informazioni proprie della lingua italiana.

Adesso siamo in grado di comprendere meglio i meccanismi linguistici e culturali, il che ci permette di creare modelli che sono in grado di farlo e di affinare gli strumenti di analisi e di moderazione, non necessariamente per censurare, ma per proteggere le persone e prevenire la violenza simbolica. I metodi computazionali da soli non bastano: devono essere integrati con un ragionamento culturale e sociale, perché l'odio implicito si nasconde proprio nei sottintesi, nelle ironie, nei silenzi, nelle cose che non si dicono.

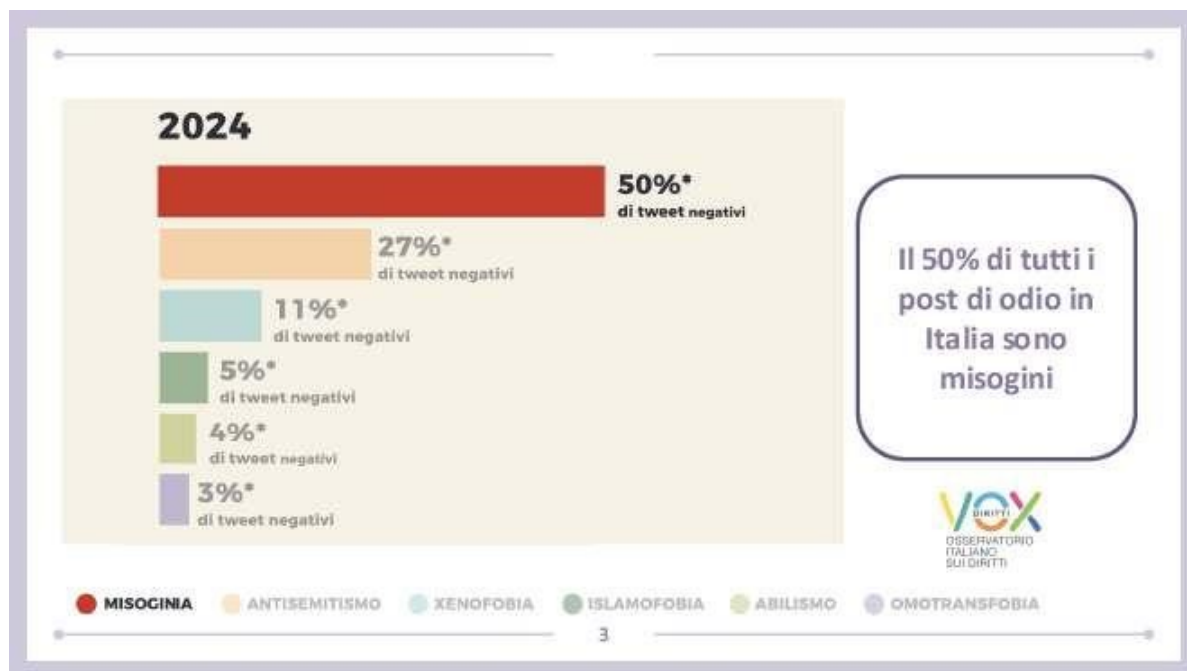
La vera moderazione non consiste solamente nel cancellare ciò che è scomodo ma nel capire il contesto e costruire contro-narrazioni che riducano il danno e cambino la cultura nell'ottica di puntare a educare le future generazioni <sup>(30)</sup>.

A lungo termine, infatti, è indispensabile un percorso di educazione digitale anche nelle scuole <sup>(31)</sup>.

Come risulta dai dati riportati nelle figure qui di seguito, il 50 per cento dei post d'odio sono caratterizzati da un contenuto misogino.

(30) Secondo *Lilia Giugni*, professoressa di Innovazione inclusiva presso l'*University College* di Londra e ricercatrice di Innovazione sociale presso l'Università di Cambridge, audita il 17 novembre 2025, la moderazione di contenuto rimane una strategia inefficiente e inefficace contro la violenza *on line*, nonché una pratica problematica sul piano etico e sociale. Questo perché, nonostante i recenti progressi nello sviluppo di *software* di moderazione automatica, supportati anche dall'intelligenza artificiale, a tutt'oggi gran parte delle operazioni di moderazione rimane affidata all'intervento umano. La moderazione delle grandi piattaforme è affidata in particolare a lavoratrici e lavoratori dislocati sul piano globale, che semplicemente non sono in condizione di gestire o di monitorare il volume e la complessità dei materiali messi *on line*, soprattutto in lingue diverse dall'inglese, come l'italiano.

(31) L'associazione « Parole O\_Stili » da anni porta avanti una campagna per far capire che nelle scuole bisognerebbe dedicare un'ora di lezione alla materia della cittadinanza digitale, « *a partire dalla prima elementare, dalla scuola primaria, perché ormai è una materia così tanto presente nella nostra vita e così talmente nuova che, assolutamente, dobbiamo diffondere l'educazione al digitale tra i bimbi e le bimbe* » (così Rosy Russo, presidente dell'associazione « Parole O\_Stili », nell'audizione del 24 novembre 2025).



## Come possiamo definire la misoginia?

*“un atteggiamento di disprezzo o avversione verso le donne, che si manifesta attraverso discriminazione, violenza, oggettificazione e esclusione dalla piena partecipazione sociale e politica” (UN Women, Glossary of Gender-related Terms, 2022).*

Esplicito

5

## Un fenomeno culturale che richiede rigore analitico

- L'AI permette di **quantificare tendenze linguistiche** e **identificare narrazioni ricorrenti**.
- L'obiettivo non è automatizzare la moderazione, ma **fornire conoscenza empirica** a supporto delle politiche pubbliche.
- L'approccio computazionale consente **trasparenza e replicabilità**, condizioni essenziali per affrontare un tema delicato come la violenza di genere.

9

Slide proiettate durante l'audizione di Debora Nozza, professoressa di Computing Sciences presso l'Università Bocconi di Milano, specializzata in elaborazione del linguaggio naturale e riconoscimento automatico della misoginia e del linguaggio d'odio on line, svolta il 20 ottobre 2025.

### 3.1.1. Le « palestre » di misoginia: gli « AI companion » o app di compagnia

Secondo Ivana Bartoletti, vicepresidente e Chief AI Governance and Privacy Officer presso Wipro Technologies e co-fondatrice del Women

*Leading in AI Network* <sup>(32)</sup>, gli *AI companion* rappresentano un pericoloso fenomeno emergente di enorme rilevanza.

Gli *AI companion* – ovvero le *app* di compagnia – sono *chatbot* avanzati basati su *Large Language Models* (LLM), modelli di intelligenza artificiale addestrati sulla base di enormi quantità di dati testuali per apprendere, sintetizzare e generare un linguaggio naturale, che vengono perfezionati attraverso l'apprendimento per rinforzo basato sul *feedback* umano <sup>(33)</sup>.

Queste tecnologie garantiscono una presenza continua e accessibile in ogni momento. L'IA non critica né dà giudizi morali e ciò favorisce un ambiente in cui le persone si sentono libere di esprimere pensieri ed emozioni, anche su temi personali o complessi.

Sono sistemi che simulano relazione, affetto, comprensione, promettono compagnia, supporto emotivo, presenza costante e ogni relazione plasma comportamenti, aspettative e modelli affettivi.

Gli *AI companions* sono quasi sempre femminili, accomodanti, docili, orientati al servizio e programmati per rafforzare dinamiche di dipendenza emotiva. Sono progettati per compiacere e si basano su ruoli stereotipati: la donna che cura, ascolta, consola e non contraddice.

Questi modelli diventano formativi, soprattutto per i ragazzi: lei non dice mai di no, lei è sempre disponibile, lei si scusa, lei perdona, lei non pone limiti. Queste dinamiche influenzano la percezione del consenso, le aspettative relazionali, la gestione delle frustrazioni e, ovviamente, la visione e il ruolo delle donne.

Gli *AI companions* possono diventare vere e proprie « palestre di misoginia ».

Quando gli utenti chiedono comportamenti sessuali estremi o violenti, i sistemi, se non sono regolati, rispondono, senza limiti, senza etica, senza correttivi.

Il rischio è duplice: la normalizzazione della violenza nelle relazioni e la creazione di dinamiche socio-digitali dove le donne sono ridotte a oggetti emotivi o sessuali programmati e programmabili.

Di qui, la necessità di garantire trasparenza, supervisione e *audit* di questi strumenti, con la creazione di *AI companions* che insegnino rispetto e parità, e un'educazione all'utilizzo della tecnologia a partire dalla scuola <sup>(34)</sup>.

(32) Audizione del 17 novembre 2025.

(33) La differenza tra *chatbot* o compagno virtuale non è immediata, ma è sostanziale, e riguarda soprattutto il modo in cui questi strumenti sono stati progettati e la loro finalità. I *chatbot* come *ChatGPT*, *Gemini* o *Claude* nascono come assistenti digitali: rispondono alle domande, chiariscono concetti complessi e, se usati responsabilmente, aiutano a lavorare meglio e in maniera più produttiva. I compagni virtuali come *Replika* o *Character.ai* hanno invece un'impostazione diversa: sono pensati per creare un legame personale ed emotivo con l'utente. Questi *bot* sono progettati per apparire vicini, empatici, quasi intimi (<https://www.gustodio.com/it/blog/compagni-ia-e-tuo-figlio/>).

(34) Gli adolescenti si affacciano alle relazioni, alle prime relazioni romantiche e alla sessualità senza parlarne con i genitori (perché si vergognano, perché i genitori stessi non iniziano il discorso), non ne parlano con i coetanei (anche qui, per non denunciare la propria inesperienza), non ne parlano a scuola e quindi si informano *on line*. C'è, quindi, un rischio di esposizione a questo tipo di contenuti. Per questo diventa fondamentale l'educazione digitale (così Giovanna Mascheroni, professoressa ordinaria di sociologia dei processi culturali e comunicativi presso l'Università Cattolica di Milano e coordinatrice di *EU Kids online* Italia, audizione del 24 novembre 2025).

#### 4. Le conseguenze della dimensione digitale della violenza contro le donne

La violenza *on line* e quella facilitata dalla tecnologia hanno un impatto devastante sulle donne, sulle ragazze e sulla società in generale.

La violenza digitale influenza ogni aspetto della vita delle vittime generando una forma di « rottura sociale » in cui la vita delle donne ha un « prima » e un « dopo » la violenza.

Le vittime, a causa delle esperienze *on line* – talvolta descritte come una « minaccia esistenziale » o un'ombra che si staglia sulla loro vita – si sentono insicure anche *off line*; si registrano danni psicologici con potenziali effetti devastanti e talvolta letali. Alla depressione, ansia, stress, paura, attacchi di panico, possono seguire anche scelte suicidarie.

La violenza digitale produce effetti negativi significativi anche a livello scolastico e professionale. A ciò si aggiunge il costo delle consulenze, delle azioni legali e degli interventi di supporto.

Rilevanti sono anche i danni relazionali e da vittimizzazione secondaria: le vittime sperimentano un profondo senso di « isolamento », vivendo abusi che distruggono la loro fiducia e i legami con la famiglia e gli amici, con il mondo *on line* e i *social media* <sup>(35)</sup>.

La diffusione della violenza digitale di genere, poi, come già ampiamente illustrato, è un danno per l'intera società, inducendo le donne ad autocensurarsi o a ritirarsi dall'impegno *on line*, limitando così la loro libertà di espressione.

#### 5. La dimensione digitale della violenza contro le donne e la valutazione del rischio nel rapporto del GREVIO

Nel monitorare l'attuazione della Convenzione di Istanbul, il GREVIO ha spesso riscontrato che la dimensione digitale della violenza contro le donne viene trascurata nelle leggi e nelle politiche nazionali <sup>(36)</sup>.

I processi di valutazione del rischio (*Risk Assessment*) spesso non includono né danno priorità all'esposizione delle donne e delle ragazze a quello *on line*, nonostante l'aumento dell'incidenza della dimensione digitale della violenza e la sua crescente criminalizzazione.

Il GREVIO ha accolto con favore il fatto che la Spagna sia stato tra i primi Paesi europei, nel 2015, a sanzionare penalmente il « *cyberstalking* », lo *stalking* perpetrato tramite mezzi di comunicazione digitali (articolo 172-ter del codice penale spagnolo).

Anche la Germania dispone di un solido quadro normativo applicabile alla dimensione digitale della violenza contro le donne, avendo sanzionato esplicitamente diverse forme di abuso facilitato dalla tecnologia, come il *cyberstalking*, l'acquisizione non autorizzata di immagini intime del corpo, la condivisione di immagini *on line* e l'uso di strumenti, programmi *software*, applicazioni e dispositivi che consen-

(35) Cfr. *The Digital Dimension of Violence Against Women as addressed by the Seven Mechanisms of the EDVAW Platform Thematic*, cit., pag. 10.

(36) Cfr. 5° Rapporto generale sulle attività del GREVIO relativo al periodo da gennaio a dicembre 2023, pag. 33 e ss.

tono di spiare segretamente la vita privata di un'altra persona attraverso il suo dispositivo mobile (c.d. *stalkerware*).

Anche l'Islanda ha assunto una posizione netta contro la violenza sulle donne *on line*: il nuovo articolo 199<sup>a</sup> del codice penale generale punisce la condivisione o diffusione di immagini intime senza il consenso della vittima. Nel febbraio 2021, è stata poi adottata la Legge sulla Protezione della *Privacy* Sessuale per rispondere alle nuove forme di violenza sessuale digitale e tutelare la libertà sessuale delle persone.

La Norvegia ha adottato una Strategia sull'abuso legato a internet (2021-2025), che si occupa dell'abuso sessuale sui bambini *on line*, e una Strategia contro i discorsi d'odio (2016-2020) per contenere anche quelli sessisti. Il Piano d'azione nazionale norvegese sulla violenza sessuale ha considerato la dimensione digitale della violenza sessuale, le diverse forme che può assumere – come la diffusione delle immagini intime e l'estorsione sessuale – e le sue caratteristiche specifiche, come l'anonimato degli autori e la natura transazionale dei reati, con un *focus* specifico sull'impatto sul benessere delle vittime<sup>(37)</sup>.

### **5.1. La Raccomandazione generale n. 1 sulla dimensione digitale della violenza contro le donne**

Il GREVIO, nella Raccomandazione generale n. 1 sulla dimensione digitale della violenza contro le donne, ha suggerito gli interventi per dare piena attuazione alla Convenzione di Budapest sulla criminalità informatica<sup>(38)</sup>, sviluppando proposte dettagliate di azione per la prevenzione di tale violenza, la protezione delle vittime e l'individuazione dei soggetti responsabili.

Viene, in particolare, raccomandato di monitorare, attraverso la raccolta di dati, il numero di suicidi, di tentativi di suicidio e di uccisione di donne e dei loro figli, correlati a molestie, *stalking* o violenza psicologica attuata attraverso strumenti virtuali.

Come osservato da *Sandra Cioffi*, presidente del Consiglio Nazionale degli Utenti<sup>(39)</sup>, l'Italia non dispone di un sistema organico, continuo e disaggregato di raccolta dati sulla violenza digitale di genere. Le informazioni disponibili sono frammentarie e questa carenza produce sottostima, ritardi di intervento e invisibilità istituzionale di una violenza che, nei fatti, anticipa, accompagna e prolunga la violenza fisica, rendendola persistente nel tempo attraverso la circolazione continua dei contenuti. Serve un sistema nazionale stabile di raccolta

(37) Il GREVIO ha apprezzato le iniziative di sensibilizzazione da parte delle Forze dell'ordine norvegesi sulla violenza di genere *on line*, consistite in conferenze nelle scuole secondarie, pubblicazione di informazioni su varie piattaforme di *social media* e la creazione di una « pattuglia della rete » in ogni distretto di polizia che offre consigli e orientamento sui reati digitali, compresi quelli a danno delle donne.

(38) Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, ratificata dall'Italia con la legge 18 marzo 2008, n. 48. La Convenzione è il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche, e tratta in particolare le violazioni dei diritti d'autore, la frode informatica, la pornografia infantile e le violazioni della sicurezza della rete. Contiene, inoltre, una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. Il suo obiettivo principale, enunciato nel preambolo, è perseguire una politica penale comune per la protezione della società contro la cybercriminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale.

(39) Cfr. memoria fatta pervenire alla Commissione il 29 gennaio 2026, pagg. 2-3.

e monitoraggio dei dati, con indicatori omogenei e disaggregati per genere, età e tipologia di violenza digitale (molestie, *cyberstalking*, *sextortion*, diffusione non consensuale di immagini intime, *hate speech* misogino), superando l'attuale frammentazione tra fonti istituzionali, Forze dell'ordine e ricerche occasionali. Serve inoltre una sempre maggiore cooperazione e *reporting* periodico da parte delle piattaforme digitali, in particolare sui contenuti di odio misogino, sulle segnalazioni di violenza di genere *on line* e sui tempi di rimozione, in raccordo con le autorità nazionali competenti.

Come anticipato, la dimensione digitale della violenza contro le donne rientra nella definizione di violenza delineata dall'articolo 3 della Convenzione di Istanbul. La norma, infatti, facendo riferimento a «*tutti gli atti di violenza di genere contro le donne che provocano, o sono suscettibili di provocare, danni o sofferenze fisiche, sessuali, psicologiche o economiche alle donne, comprese le minacce di tali atti, la coercizione o la privazione arbitraria della libertà, sia in contesti pubblici sia privati*», comprende anche la condivisione non consensuale di immagini o video, la coercizione, le minacce, comprese quelle di stupro, il bullismo sessualizzato, le molestie sessuali *on line*, il furto di identità, lo *stalking on line* o tramite l'*Internet of Things* (IoT)<sup>(40)</sup>.

L'articolo 5, paragrafo 2, della Convenzione di Istanbul impone agli Stati Parte l'adozione delle necessarie misure, non solo legislative per prevenire, indagare, punire e garantire tutela alle vittime in presenza di violenza di genere. Si tratta di un obbligo di mezzi, non di risultati. Per il GREVIO, questo obbligo riguarda tutte le forme di violenza contro le donne, comprese le espressioni digitali e la violenza commessa con l'ausilio o tramite la tecnologia, per le quali, ad oggi, non si è ancora in grado di garantire che i responsabili rispondano delle proprie azioni<sup>(41)</sup>.

Uno dei presupposti della Convenzione di Istanbul è assicurare una risposta globale a tutte le forme di violenza contro le donne e alla violenza domestica, offrendo un insieme di politiche efficaci, comprensive e coordinate a livello statale e una pluralità di misure che coinvolgano diversi attori, agenzie e parti interessate.

Quanto, in particolare, alla dimensione digitale della violenza contro le donne, occorrono politiche comprensive che includano e affrontino specificamente queste forme di violenza sotto il profilo della prevenzione, del sostegno e della protezione delle vittime e dell'azione penale<sup>(42)</sup>, considerata la complessità e la natura multidimensionale del problema.

(40) L'IoT è la rete di oggetti fisici connessi tra loro e con internet in grado di registrare e trasmettere dati sul loro utilizzo.

(41) Per il Commissario del Consiglio d'Europa per i Diritti Umani, la mancanza di consapevolezza su questo tema fa sì che gli attacchi informatici e la violenza contro le donne non vengano presi con la stessa serietà della violenza *off line* dalle autorità nazionali. Le Forze dell'ordine e le autorità giudiziarie spesso non dispongono della formazione tecnica necessaria per poter investigare e perseguire efficacemente tali episodi di violenza (<https://www.coe.int/it/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world>).

(42) Per Simona Lanzoni, vicepresidente della fondazione Pangea Onlus, audita il 10 novembre 2026, il problema è la questione della territorialità del reato: «*perché l'on line non ha spazio, non ha geograficamente un'identificazione possibile e neanche una temporalità determinata. A un certo punto, quindi, diventa un vero problema. Quello che noi vediamo è un problema, nel momento in cui si va a denunciare, di identificazione della*

Come la violenza *off line*, quella *on line* è profondamente radicata nelle dinamiche di potere, negli squilibri economici che alimentano l'idea dell'inferiorità delle donne rispetto agli uomini. Fondamentale, pertanto, è che all'intervento del legislatore si affianchi un cambiamento culturale su larga scala.

Il fenomeno della violenza di genere ha un aspetto irriducibilmente culturale che non può essere soltanto prevenuto e contrastato attraverso la risposta securitaria, che pure è una risposta indispensabile <sup>(43)</sup>.

## 6. Le principali forme di violenza digitale

### 6.1. Condivisione non consensuale di immagini intime

Con il termine « *revenge porn* » si fa generalmente riferimento al fenomeno della diffusione non consensuale di immagini o video dal contenuto sessualmente esplicito di una persona o della minaccia di condivisione. Il fenomeno comprende gli atti di « *upskirting* » <sup>(44)</sup> e di « *creepshot* » <sup>(45)</sup>, oltre all'acquisizione di immagini in maniera fraudolenta (con videocamere nascoste) oppure la produzione digitale di immagini alterate ricorrendo a sistemi di intelligenza artificiale (*deepnude*) <sup>(46)</sup>.

### 6.2. Molestie sessuali

Il bullismo a sfondo sessuale è un comportamento prevaricante e intimidatorio che ha a che fare con la sfera sessuale o con dinamiche di tipo sessuale. Consiste nella diffusione di pettegolezzi o voci sulle abitudini sessuali di una persona, nella pubblicazione di commenti a sfondo sessuale sotto i post o le foto della stessa sui *social* o nell'assunzione della sua identità al fine di condividere, a suo nome, contenuti sessuali o molestare sessualmente terzi, facendo ricadere la colpa sulla

---

*territorialità del reato, ma anche di conoscenza sufficiente della pervasività delle possibilità di fare violenza on line. Abbiamo, quindi, una mancanza di proattività, per esempio di emissione di misure cautelari, e difficoltà a fare investigazioni che possano realmente arrivare a identificare dove sia il maltrattante e che cosa stia realmente facendo. È come avere una matita con la mina spuntata: non si riesce veramente ad agire ».*

(43) Sono le parole del Prefetto Bruno Frattasi, direttore dell'Agenzia per Cybersicurezza Nazionale, che, nel corso dell'audizione del 6 novembre 2025, ravvisando l'origine del problema in « *un fatto di educazione, di cultura, cultura che subisce quel fenomeno, più volte osservato, anche recentemente, da sociologi e politologi, che si chiama "deculturazione" del mondo* », ha invocato la costruzione di « *una cittadinanza digitale responsabile e consapevole* ». Per Letizia Basile, presidente della associazione di promozione sociale, « *Iostaccolaspina Aps* », nell'audizione del 12 febbraio 2026, la risposta repressiva deve essere accompagnata da « *una strategia strutturata di prevenzione in grado di intervenire in una fase precoce* ».

(44) L'*upskirting* (dall'inglese *up*: su e *skirt*: gonna) è una forma di molestia sessuale che consiste nel riprendere, tramite una fotocamera o una telecamera posizionata sotto la gonna, la parte inferiore della figura femminile mettendone in evidenza la biancheria intima o la nudità. Tali immagini vengono spesso diffuse *on line* senza il consenso delle vittime anche minorenni.

(45) I *creepshots* sono foto « *sessualmente suggestive* » di donne scattate senza il loro consenso.

(46) Come spiegato da Lucia Bainotti, Assistant Professor in Digital and Visual Media Analysis presso il Dipartimento di Media Studies dell'Università di Amsterdam, audita il 17 novembre 2025, queste condotte rientrano nelle cosiddette « *forme di abuso attraverso l'immagine* », dall'inglese *image-based sexual abuse*, che si riferiscono esattamente a delle forme che avvengono attraverso il mezzo digitale.

ignara vittima. Ciò determina un pesante danno di immagine e di reputazione. Nel fenomeno rientra anche la condotta di rivelazione delle inclinazioni sessuali di taluno (c.d. «outing») senza il suo consenso al fine di spaventarlo, ricattarlo e umiliarlo.

### 6.3. Cyberstalking

Come ricordato dal Dirigente superiore della Polizia di Stato *Ivano Gabrielli*, Direttore del Servizio Polizia postale e per la sicurezza cibernetica <sup>(47)</sup>, l'uso della tecnologia ha, di fatto, ampliato la portata del fenomeno dello *stalking*, che comprende comportamenti offensivi o minacciosi reiterati nei confronti di una vittima attuati *on line* mediante l'invio sistematico di messaggi, la pubblicazione di commenti, il monitoraggio da remoto e il tracciamento dei dati, anche utilizzando *account* falsi e *stalkerware*, che permettono di spiare la vita della vittima, o mediante la clonazione del suo dispositivo attraverso una *app* spia (applicazioni che operano in modalità *stealth* <sup>(48)</sup>).

Il *cyberstalker* segue ripetutamente un'altra persona o intrattiene, con la stessa, comunicazioni indesiderate <sup>(49)</sup> o le fa sapere che la sta osservando. L'autore del reato segue ovunque la vittima, apparendo nel luogo di lavoro, nelle strutture sportive, ricreative o educative e anche nel mondo virtuale (*chat room*, siti di *social networking*, ecc.).

Gli atti persecutori nella sfera digitale includono minacce (di natura sessuale, economica e fisica), prospettazione di danni alla reputazione, monitoraggio e raccolta di informazioni private, furto di identità, richiesta di atti sessuali e molestie anche attraverso complici così da isolare la vittima. Lo *stalker* sorveglia, spia la vittima, i suoi profili sui *social media*, le applicazioni di messaggistica, le *email* e il telefono, sovente rubando la *password* o violando o «hackerando» i dispositivi per accedere agli spazi privati, tramite l'installazione di *spyware* o *app* di geolocalizzazione <sup>(50)</sup>. Può anche capitare che gli autori di queste condotte assumano l'identità della vittima o riescano a monitorarla tramite dispositivi tecnologici collegati attraverso l'*Internet of Things (IoT)*, come elettrodomestici intelligenti.

(47) Audizione 17 novembre 2025.

(48) In modalità invisibile, nascosta.

(49) Partecipare a comunicazioni indesiderate implica la ricerca di qualsiasi contatto attivo con la vittima attraverso qualsiasi mezzo di comunicazione disponibile, inclusi strumenti di comunicazione moderni e dispositivi di telecomunicazione.

(50) La geolocalizzazione è il processo di determinazione della posizione geografica esatta di una persona, di un dispositivo o di un oggetto. La portata del fenomeno, soprattutto tra i giovanissimi, è stata rappresentata da *Maura Manca*, presidente dell'Osservatorio Nazionale Adolescenza Onlus, che nel corso dell'audizione del 3 dicembre 2025, ha raccontato che: «L'insicurezza, la gelosia ci può anche stare, è normale, è un sentimento tra adulti, tra ragazzi. Soprattutto loro, che sono in fase di crescita, hanno tantissimi cambiamenti dal punto di vista emotivo da affrontare: relazionale, di identità, di paura, di confronto. È normale, anzi la gelosia, l'insicurezza può portare anche, se hanno gli strumenti giusti, a parlare tra loro, interagire e costruire una connessione più profonda. Si può anche parlare delle proprie insicurezze, delle proprie paure e anche delle proprie gelosie. Quando io arrivo a doverti anche geolocalizzare per stare tranquillo, a dover sapere sempre dove sei, cosa scrivi, cosa fai, creare profili falsi per poter vedere come rispondi, come interagisci, è vivere tutto il giorno per controllare anche le tue attività, significa che vengo meno anche in funzione della mia stessa vita e che sto normalizzando un concetto di amore che non è amore».

#### 6.4. La violenza psicologica *on line*

La violenza psicologica *on line* può assumere anche la forma di intimidazione, minacce rivolte alle vittime o ai loro congiunti, insulti, discredito e diffamazione.

L'istigazione al suicidio o agli atti autolesionistici è un comportamento specifico che si manifesta *on line*, spesso amplificato dai meccanismi della mentalità di gruppo e dell'anonimato<sup>(51)</sup>.

#### 6.5. L'abuso economico

Un'altra forma di violenza psicologica è l'abuso economico, definito come il controllo della capacità di una donna di acquisire, utilizzare e mantenere risorse economiche.

L'abuso economico solitamente matura nel contesto della violenza tra partner intimi e produce effetti negativi sulla salute fisica delle vittime, limitando l'accesso alle cure sanitarie. Minacciando il benessere finanziario e l'indipendenza economica della vittima, influisce in modo grave sulla sua integrità psicologica.

Si tratta di un modello di comportamento di controllo, minaccia e degrado che limita la libertà. L'obiettivo è lasciare la vittima senza soldi, disorientata e insicura così da poterla controllare meglio. Di fatto è l'atto con cui l'abusante, il partner, utilizza il denaro come strumento ricattatorio, per rendere la vittima impotente, dipendente e facilmente controllabile.

L'abuso economico spesso si accompagna al cosiddetto *gaslighting*<sup>(52)</sup>.

La vittima, resa insicura dalle denigrazioni sistematiche messe in atto dal partner, alimenta, essa stessa, la spirale del controllo. L'inevitabile isolamento dal mondo del lavoro e dal resto della comunità, poi, concorre a fare il resto. L'abusata si convince di non essere in grado di farcela da sola e non trova il coraggio di interrompere la relazione. E tutto ciò avviene, quasi sempre, senza che se ne renda veramente conto, fino a quando non si palesa la violenza fisica, più facilmente riconoscibile<sup>(53)</sup>.

Nei *forum* digitali, l'abuso economico può manifestarsi con il controllo dei conti correnti bancari e delle attività finanziarie tramite

(51) Rosanna Milone, responsabile progetti e *Awareness and Advocacy Strategist* della Fondazione Carolina, nel corso della audizione del 24 novembre 2025, ha spiegato che Fondazione Carolina è nata in memoria di una ragazza alla quale è stato fatto un video mentre era in stato di semincoscienza. Questo video è diventato virale ed è stata attaccata *on line*, finché non è crollata e ha deciso di suicidarsi. Nella lettera che ha scritto prima di compiere questo gesto terribile ha lasciato messaggi molto forti: ha detto che le parole fanno più male delle botte e auspicava anche che ciò che era accaduto a lei non accadesse più a nessuno. In seguito alla sua morte si è svolto il primo processo di cyberbullismo in Italia e abbiamo già sentito che in suo onore è stata anche varata la prima legge, non solo in Italia, ma in Europa, sul cyberbullismo.

(52) Il *gaslighting* è una tecnica di manipolazione psicologica che porta la vittima a dubitare della realtà e può avere conseguenze profonde sul suo benessere emotivo e mentale. Il termine deriva dal film «*Gaslight*» del 1944, diretto da George Cukor, che narra la storia di Paula, interpretata da Ingrid Bergman, vittima di manipolazione psicologica da parte del marito Gregory, interpretato da Charles Boyer. Il marito altera le luci della lampada a gas nella loro casa, facendo credere a Paula di essere vittima di allucinazioni, portandola a dubitare della sua percezione della realtà e della sua salute mentale.

(53) <https://www.lofficinadelrisparmio.it/abuso-economico/>.

il *banking on line*, facendo venir meno l'affidabilità creditizia della vittima per effetto dell'uso di carte di credito senza autorizzazione o l'intestazione di tutti i contratti (di finanziamento, di mutuo, delle utenze, ecc.) a suo nome senza poi procedere al pagamento<sup>(54)</sup>.

#### 6.6. Il *child grooming*

Con i termini «*grooming*» o «*child grooming*» si suole indicare la condotta di adescamento<sup>(55)</sup>. Il verbo «*to groom*» significa avere cura, tenere pulito, ordinato. Chi adesci, però, non si prende cura della vittima ma della costruzione della relazione di fiducia con stessa, una fiducia funzionale all'acquisizione di confidenze e informazioni sensibili da utilizzare, poi, nella fase successiva del ricatto, quando il minore cercherà di sottrarsi alle prime richieste di natura sessuale<sup>(56)</sup>.

Solitamente chi adesci i minori è una persona da questi frequentata o che frequenta spesso i luoghi dove si trovano bambini e ragazzi, come scuole, centri sportivi, parchi gioco. Ma l'adescatore può anche operare *on line*, dove l'anonimato e la circostanza che i bambini e i ragazzi vengono lasciati soli a usare *social network* e *app* gli consentono di operare senza il timore che qualche adulto di riferimento possa intervenire.

Come ha spiegato Cristina Obber, scrittrice e giornalista, «*per diventare amici servono pazienza e tempo, affinché il minore sia successivamente ricattabile. Questo tempo viene proprio utilizzato per raccogliere il maggior numero di informazioni sensibili, utili anche per poterlo poi incontrare personalmente e agire, quindi, un abuso di contatto. Dobbiamo abbandonare lo stereotipo del pedofilo anziano e solitario, con poche relazioni sociali. Molti di loro non sono pedofili (ossia non hanno un interesse sessuale esclusivo per i minori), molti hanno meno di trent'anni, ma sono in crescita anche gli adescatori minorenni, che hanno altri obiettivi e motivazioni, però ugualmente lesivi della dignità della salute mentale e sessuale delle vittime. Gli adescatori sono uomini comuni, con la stessa eterogeneità e trasversalità che incontriamo nel femminicidio e nella violenza sessuale, che ben conoscete. Io mi riferisco al maschile perché gli studi in materia ci parlano prevalentemente di autori maschi. Esiste una presenza femminile irrisoria, che è comunque oggetto di studio perché è anche più difficile da identificare, ma anche in questo tipo di violenza c'è di mezzo il potere, c'è di mezzo il controllo, quindi il genere conta*»<sup>(57)</sup>.

Le vittime non sono solo minori che presentano particolari vulnerabilità, fragilità, o che vengono da contesti familiari o sociali di

(54) GREVIO, *General Recommendation No. 1 on the Digital Dimension of Violence Against Women*, cit. pag. 19.

(55) Particolare preoccupazione desta l'aumento di: *grooming on line*, ossia adescamento di minori spesso realizzato attraverso *chat*, *social network* e piattaforme di *gaming*; scambio di materiale sessualmente esplicito, utilizzato come strumento di ricatto (Sandra Cioffi, presidente del Consiglio Nazionale degli Utenti, memoria del 29 gennaio 2026, cit., p. 5).

(56) La definizione criminologica che riferisce il Dizionario di Cambridge del verbo «*to groom*» è la seguente: «diventare amico di un bambino con l'intenzione di cercare di convincerlo ad avere una relazione sessuale». Marina Terragni, Garante per l'Infanzia e l'Adolescenza, nella relazione trasmessa in data 9 febbraio 2026, parla di una «modalità predatoria messa in atto da persone adulte nei confronti di persone minori».

(57) Audizione del 10 novembre 2025.

particolare disagio: chiunque può essere adescato, perché le tecniche di manipolazione psicologia sono sempre più sofisticate. Possono durare settimane o anche mesi, senza che venga inserito nella conversazione un elemento a connotazione sessuale. Le difese dei minori, ben consapevoli dei rischi che corrono *on line*, si abbassano, perché c'è una falsa percezione di intimità dovuta al luogo in cui avviene l'adescamento: la cameretta, dove ci si sente al sicuro.

I numeri, seppur già allarmanti, che troviamo nei preziosi rapporti della Polizia postale<sup>(58)</sup>, fotografano solo una minima parte del fenomeno. Nella maggior parte dei casi gli adescatori non vengono individuati grazie alle denunce delle famiglie delle vittime ma dalle indagini sotto copertura che gli agenti delle Forze dell'ordine conducono nelle reti, nei gruppi di scambio e commercializzazione di materiale pedopornografico. Una volta intercettato un adescatore, dall'esame dei suoi dispositivi si riesce a risalire a tutte le sue vittime che, in quel momento, stanno subendo e soffrendo in solitudine, all'insaputa dei familiari.

### 6.7. L'orbiting

L'*orbiting*<sup>(59)</sup> è un comportamento digitale diventato popolare sul *web* e sui *social* in cui una persona, dopo aver iniziato una relazione virtuale o un contatto, dirada sempre di più i rapporti, continuando tuttavia a « orbitare » intorno all'altro attraverso i *social media*, ad esempio visualizzando storie, mettendo i *like* o commentando saltuariamente, senza però stabilire un'interazione diretta. Mantiene, dunque, un contatto, seppur virtuale, senza mai sviluppare una relazione significativa o approfondire la conoscenza. Questo comportamento appare ambiguo e poco trasparente perché crea l'illusione di un interesse sentimentale, quando in realtà non c'è nulla di concreto.

Alla base di questo comportamento vi è una profonda insicurezza, una paura del distacco e un bisogno di esercitare un controllo sull'altro;

(58) Il Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO) – istituito dall'articolo 19 della legge 6 febbraio 2006, n. 38, in materia di Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo internet – ha confermato nel 2025 un ruolo centrale nella tutela dei minori e delle persone vulnerabili – supportato anche dall'attività dell'Unità di Analisi del Crimine Informatico, *équipe* di funzionari psicologi della Polizia di Stato – con un'azione operativa concentrata su attività mirate e qualitative. Nel 2025 i procedimenti per pedopornografia e adescamento sono stati 2.574, con 222 arresti. Il monitoraggio dei contenuti CSAM (*Child Sexual Abuse Material*, ovvero materiale pedopornografico o materiale relativo ad abusi sessuali su minori) ha riguardato oltre 16.500 siti, con 2.876 inserimenti in *black list*, privilegiando indagini su aree oscure della rete e piattaforme criptate. La Sezione Operativa, impegnata nella tutela della persona dai reati commessi *on line*, ha svolto un'azione che si è tradotta in 1.298 persone indagate e 245 perquisizioni, a testimonianza di un impegno operativo costante, multidisciplinare e orientato alla tutela concreta delle persone, con particolare attenzione alle diverse forme di aggressione riconducibili alle fattispecie previste dal cosiddetto « Codice Rosso ». I fenomeni dello *stalking*, delle molestie *on line* e della diffusione illecita di immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, presentano una marcata connotazione di genere, colpendo prevalentemente le donne. Nel corso del 2025 sono state attivate 477 procedure di Codice Rosso, in prevalenza per casi di *stalking* e *revenge porn*.

(59) Dall'inglese « *orbitare attorno a qualcosa* », il termine « *orbiting* » descrive una modalità relazionale che può verificarsi nelle interazioni *on line*.

chi ne è vittima può arrivare a mettere in dubbio sé stesso, provando sensazioni di inadeguatezza e disistima<sup>(60)</sup>.

### 6.8. Il *ghosting*

Il *ghosting* – letteralmente, « sparire come un fantasma » – rappresenta un fenomeno sempre più diffuso, favorito dalle nuove tecnologie della comunicazione.

Nell'era digitale, avere un profilo *social* aggiornato e dare testimonianza delle proprie attività quotidiane è la normalità. Eppure, nelle relazioni interpersonali una tendenza attuale e sempre più diffusa è quella di porre fine a un rapporto senza dare alcuna spiegazione.

Tipicamente, in questo tipo di comportamento, dopo un periodo di frequentazione (anche intensa), all'improvviso, chiamate e messaggi restano senza risposta e si perde quasi ogni traccia dell'altra persona. La diffusione di questa pratica è dovuta, tra le altre cose, alla facilità con cui è possibile « sparire nel nulla ».

Questo comportamento può lasciare chi lo subisce in uno stato di sospensione emotiva, alimentando: ansia e confusione (« ho fatto qualcosa di sbagliato ? »); abbassamento dell'autostima (« non valgo abbastanza da meritare una spiegazione »); rabbia e senso di ingiustizia<sup>(61)</sup>.

Non è raro, poi, che il/la *ghoster* blocchi l'altra persona su tutti i *social network*<sup>(62)</sup>.

### 6.9. Il *sexting*

Il *sexting*<sup>(63)</sup> consiste principalmente nello scambio di messaggi sessualmente espliciti e di foto e video a sfondo sessuale, spesso realizzate con il telefono cellulare, o nella pubblicazione per via telematica, attraverso canali come *chat*, *social network*, *internet* e varie *app*.

L'iscrizione massiccia ai *social network* e alle piattaforme di messaggistica ha contribuito alla massiccia diffusione del *sexting*, facili-

(60) <https://www.riza.it/psicologia/coppia-e-amore/8365/orbiting-significato-caratteristiche-cause-e-cosa-fare.html>. Osserva l'avvocato Elisabetta Aldrovandi, collaboratrice esterna della Commissione, nella memoria depositata presso la Commissione il 2 marzo 2026, che tale comportamento può « costituire contesto di condotte più gravi (stalking, cyberstalking, molestie reiterate, atti persecutori) con impatto sulla salute psicologica, specie su giovani donne, in un ecosistema digitale già connotato da asimmetrie di potere ».

(61) <https://www.rabuffi.it/it/psicologo-milano/ghosting-di-cosa-si-tratta-e-come-protegersi>. Il *ghosting* interrompe bruscamente il legame: il cervello interpreta il silenzio improvviso come una perdita reale e si attiva un dolore emotivo simile a quello del lutto. Senza spiegazioni, la mente continua a cercare risposte e fatica ad andare avanti. Il *ghosting* colpisce poi l'autostima in quanto il messaggio implicito che trasmette è: « non meriti nemmeno una parola ».

(62) <https://www.santagostino.it/magazine-psiche/ghosting/>.

(63) Si tratta di un neologismo derivato dalla fusione delle parole inglesi *sex* (sesso) e *texting* (inviare messaggi elettronici). Secondo Ernesto Caffo, « molti di questi materiali di *sexting* sono prodotti dagli stessi ragazzi. Questo aspetto, associato allo scambio, anche economico, attorno a queste immagini, può determinare un'area di grandissimo rischio, su cui dobbiamo assolutamente intervenire. In questi casi c'è bisogno, da una parte, di poter dare un aiuto alla vittima e, dall'altra parte, di poter avere strumenti di intervento, come lo abbiamo noi, come Telefono Azzurro, nel ruolo di *trusted flagger*, per poter intervenire sulle piattaforme per togliere questo materiale. L'esposizione di questi video, che diventano virali immediatamente nella rete, porta sulle vittime conseguenze particolarmente significative » (audizione del 17 dicembre 2025).

tando l'invio di video e di foto sessualmente esplicite. Il fenomeno è diventato molto comune in particolare tra gli adolescenti. Le immagini, anche se inviate in origine a una ristretta cerchia di persone, si possono diffondere in seguito in modo incontrollabile con gravi danni per la reputazione della persona ritratta.

Si è soliti classificarlo in tre tipologie:

- 1) scambio di immagini e testi solamente tra due *partner*;
- 2) scambi di immagini e testi che non coinvolgono solo i due partner ma sono condivisi con altri soggetti estranei alla relazione;
- 3) scambi di immagini e testi tra soggetti che non intrattengono ancora una relazione ma dove almeno una delle due parti desidera averla.

#### 6.10. Le ulteriori forme

L'attacco DDoS (*Distributed Denial of Service*, « attacco distribuito di negazione servizio ») è un tentativo di sovraccaricare e interrompere o disabilitare un servizio o un *server*, inondandolo con più traffico internet di quanto sia in grado di gestire <sup>(64)</sup>.

Con il termine *hacking* si indica il processo per ottenere l'accesso a un sistema informatico o a una rete in modo illegale o senza consenso.

L'*happy slapping* (letteralmente « schiaffeggio allegro ») è l'atto di attaccare (fisicamente o sessualmente) una persona con l'obiettivo di filmare l'aggressione e condividerla *on line* <sup>(65)</sup>. Il video, una volta divulgato, diventa immediatamente virale – per effetto della condivisione da parte di un numero indefinito di utenti – e oggetto di commenti offensivi.

L'*outing* consiste nel rivelare l'orientamento sessuale o l'identità di genere di qualcuno senza il suo consenso, spesso in modo pubblico. A differenza del *coming out*, che è un processo volontario e positivo, l'*outing* è un atto che può essere percepito come aggressivo e invasivo.

L'estorsione sessuale (*sextortion*) è la minaccia di pubblicare contenuti sessuali (immagini, video, *deepnude*, notizie sulla sfera sessuale) per intimidire o costringere qualcuno ad inviare altri contenuti a sfondo sessuale e/o somme di denaro. Il fenomeno si è evoluto

(64) L'aggressore hacker computer o altri dispositivi e installa un codice malevolo, o *malware*, chiamato *bot*. Insieme, i computer infetti formano una rete chiamata *botnet* alla quale l'aggressore chiede di sovraccaricare i *server* e i dispositivi della vittima con più richieste di connessione di quelle che è capace di gestire.

(65) Si tratta della cosiddetta violenza performativa. Viviamo in un'epoca che impone di « essere qualcuno » a tutti i costi. In questo contesto, l'atto violento si trasforma in un rito di auto-affermazione per uscire dall'anonimato e sentirsi, per un istante, potenti e visibili. Questa dinamica oggi trova la sua massima espressione nella dimensione digitale: l'aggressione spesso non serve a risolvere un conflitto, ma a creare un contenuto. Filmare una rissa con lo *smartphone* non è un gesto accessorio, ma il fine ultimo dell'azione. L'atto esiste solo se viene condiviso e validato dai « *like* » di una platea virtuale, trasformando il corpo della vittima in un semplice oggetto di scena deumanizzato. Dove la violenza è performativa, la prevenzione deve passare per una nuova alfabetizzazione digitale: è fondamentale insegnare ai giovani che la viralità non è identità e che la sofferenza altrui non può essere ridotta a un contenuto per ottenere « *like* » (Violenza giovanile in Italia: dati, cause profonde e perché i casi sono in aumento – CIAI, news dell'11 febbraio 2026, in <https://www.ciai.it/violenza-giovanile/>).

parallelamente al diffondersi del « *sexting* », in cui immagini e video espliciti vengono condivisi, da un individuo ad un altro, senza una reale consapevolezza delle conseguenze, a breve e a lungo termine, della trasmissione di contenuti « privati » su strumenti digitali progettati per la ricondivisione.

Con il termine *swatting*<sup>(66)</sup> si fa riferimento all'uso di telefoni – e spesso di sistemi informatici – per ingannare un servizio di emergenza sulla base di una segnalazione falsa. Gli *swatter* possono segnalare un falso allarme bomba, una situazione di ostaggio, una attività terroristica o un omicidio. Le minacce *swatting* sono in genere fatte in forma anonima o attraverso false identità.

Il *trolling*<sup>(67)</sup> consiste nel pubblicare deliberatamente commenti offensivi *on line*, a volte con l'esplicita intenzione di causare allarme, disagio o umiliazione. Un *troll*, nel gergo di internet e, in particolare, delle comunità virtuali, è un soggetto che interagisce con gli altri tramite messaggi volutamente provocatori, irritanti, fuori tema o semplicemente senza senso e/o del tutto errati, con il solo obiettivo di disturbare la comunicazione e causare nervosismo. Gli attacchi possono anche essere portati a segno da un gruppo di persone in modo coordinato e mirato<sup>(68)</sup>.

Il *fraping*<sup>(69)</sup> è l'accesso non autorizzato a un *account* di un *social media*, finalizzato alla pubblicazione di contenuti imbarazzanti o dannosi. Questa condotta viola l'identità personale della persona colpita che, sovente, viene colpevolizzata per non aver protetto adeguatamente la propria *privacy*.

L'*hate speech* fa riferimento a ogni comunicazione che incita all'odio, alla violenza o alla discriminazione contro persone o gruppi<sup>(70)</sup>.

La possibile relazione causale tra espressioni d'odio e crimini d'odio che sfociano in azioni di violenza fisica comporta che si debba prestare particolare attenzione alla raccolta dei dati relativi alle espressioni d'odio, non solo con riferimento ai singoli individui che se ne facciano portatori, ma anche al loro precipitare nel discorso pubblico, anche ad opera di chi detenga, a vario titolo, responsabilità editoriali,

(66) Il nome deriva da SWAT, acronimo inglese per *Special Weapons And Tactic*, che è una squadra appositamente addestrata per rispondere a eventi potenzialmente pericolosi, come una situazione che può coinvolgere ostaggi.

(67) Il termine deriva dal norvegese « *troll* », che indicava originariamente una creatura leggendaria dalle sembianze mostruose, spesso associata alla magia e alle forze della natura.

(68) *Annex: Glossary*, in *GREVIO General Recommendation No. 1 on the Digital Dimension of Violence Against Women*, cit. pagg. 19 e 25.

(69) Il termine deriva dalla combinazione di « *Facebook* » e « *rape* » (stupro in inglese) e descrive l'azione di chi accede senza consenso al profilo di una persona su *Facebook*, manipolando le informazioni personali e pubblicando messaggi falsi.

(70) *Barbara Giovanna Bello*, ricercatrice e docente di filosofia del diritto e di giustizia digitale presso l'Università degli Studi della Tuscia, nel corso dell'audizione del 4 febbraio 2026, ha fatto notare che il codice penale, agli articoli 604-bis e 604-ter, prevede il discorso d'odio (comunemente chiamato « *hate speech* »), ma non include il motivo sessista, non include l'odio basato sul genere. « *Questa credo sia una importante integrazione e credo che i tempi siano propizi per poter procedere a questa integrazione, se non altro perché, ricorrendo alla famosa piramide dell'odio ideata dalla Anti Defamation League, notiamo che alla base ci sono gli stessi pregiudizi, gli stessi stereotipi che si esprimono attraverso il linguaggio dell'odio e il linguaggio discriminatorio, per poi, in una escalation sempre crescente, diventare attacchi alla persona e alle cose, per poi arrivare all'apice della piramide, ossia all'annichilimento della persona, quindi all'uccisione, all'esclusione totale della persona. Ecco: agire sui reati cosiddetti "sentinella" può espletare l'effetto di prevenire proprio quella escalation* »..

politiche o istituzionali e si esprima in pubblico attraverso i diversi mezzi di comunicazione di massa.

Le forme di discorso d'odio sui *social* possono manifestarsi attraverso messaggi, *post*, immagini, *meme* <sup>(71)</sup> con esplicita finalità denigratoria <sup>(72)</sup>. Per diverse ragioni, comunque, gli ambienti digitali sembrerebbero più predisposti al proliferare di offese, toni esasperati e provocatori, atteggiamenti irrispettosi e discriminanti.

Una delle principali ragioni è costituita dall'anonimato che caratterizza questo tipo di ambienti: quando ci si nasconde dietro il *nick* e l'*avatar* di un profilo *social*, si hanno meno remore nell'esprimere anche le posizioni più estreme e meno *politically correct*.

Gli utenti, poi, tendono a sottostimare gli effetti concreti che ciò che avviene in rete può avere nella realtà.

---

(71) Un *meme* – o, meglio, un internet *meme* – è un contenuto di natura umoristica o frutto di rielaborazione creativa di scene di film, serie o programmi TV, opera artistiche diventati cult nell'immaginario comune che si diffonde rapidamente in rete diventando virale.

(72) Nonostante oggi l'espressione venga usata per lo più con riferimento all'*internet hate speech* (o *on line hate speech*), il fenomeno preesiste alla rete. La possibilità di cadere nel discorso dell'odio, del resto, è da sempre un rischio concreto quando ci si confronta con gli altri all'interno di uno spazio o dibattito pubblico (<https://www.insidemarketing.it/glossario/definizione/hate-speech/>).

## Parte I LA TUTELA CIVILISTICA DELLE IMMAGINI DELLE PERSONE

### 1. La tutela civile

#### 1.1 Il fondamento normativo

La tutela dell'immagine della persona si rinviene nell'articolo 10 del codice civile e anche negli articoli 96 e 97 della legge 22 aprile 1941, n. 633 (legge sul diritto di autore).

Con l'articolo 10 del codice civile il legislatore offre una specifica disciplina per l'ipotesi di abuso dell'immagine, prevedendo che *« qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni »*.

L'articolo 96, primo comma, della citata legge n. 633 del 1941 stabilisce, poi, che *« il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa, salve le disposizioni dell'articolo seguente »*<sup>(73)</sup>.

Tale regola subisce un'eccezione nel momento in cui la pubblicazione è giustificata dalla notorietà della persona ritratta o quando è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico. In particolare, ai sensi dell'articolo 97 della legge n. 633 del 1941, *« non occorre il consenso della persona ritrattata quando la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali, o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico. Il ritratto non può tuttavia essere esposto o messo in commercio, quando l'esposizione o messa in commercio rechi pregiudizio all'onore, alla reputazione od anche al decoro della persona ritrattata »*.

Il divieto è assoluto nella ipotesi in cui l'esposizione o la pubblicazione rechi pregiudizio all'onore, al decoro o alla reputazione della persona ritratta, perché in questa ipotesi l'esigenza del rispetto dell'intimità della persona prevale sull'esigenza sociale di pubblica conoscenza della sua immagine, sicché non sono ammesse deroghe al divieto di divulgazione.

Il diritto all'immagine – configurato in dottrina talora come manifestazione del più ampio diritto alla riservatezza, talaltra come autonomo diritto della personalità – ha un duplice contenuto, negativo e positivo. Sotto il primo profilo, il diritto tutela l'interesse del titolare

(73) La norma, nell'esigere il consenso della persona ritratta per la esposizione riproduzione o messa in commercio del ritratto, salve le ipotesi di cui all'articolo successivo, non prevede particolari forme per la sua manifestazione ammettendo pertanto anche che esso possa essere manifestato tacitamente (Cass. civ. n. 5175 del 1997; Cass. civ. n. 3014 del 2004; Cass. civ. n. 11491 del 2006; Cass. civ. n. 21995 del 2008). Il consenso, la c.d. liberatoria all'uso dell'immagine, può quindi essere anche tacito, purché risulti da una manifestazione di volontà sufficientemente concludente (in questo senso Cass. civ. 36754 del 2021).

a che la sua immagine non venga diffusa o esposta in pubblico; la correlativa situazione giuridica soggettiva passiva posta in capo alla totalità (*erga omnes*) dei consociati consiste in un dovere di astensione<sup>(74)</sup>. Sotto il secondo profilo, il diritto tutela l'interesse del titolare ad apparire in pubblico nella misura in cui abbia interesse a farlo; la correlativa situazione giuridica soggettiva passiva posta in capo alla totalità (*erga omnes*) dei consociati consiste in un obbligo di *pati*<sup>(75)</sup>.

## 1.2 La rilevanza costituzionale

Il diritto alla protezione dell'immagine personale è considerato dalla maggioranza degli interpreti come manifestazione del più ampio diritto alla riservatezza.

Com'è noto, tale diritto non è espressamente menzionato nella Costituzione ma è stato desunto dall'interpretazione sistematica di altre norme della Carta fondamentale, come ad esempio l'articolo 13 sulla libertà personale, l'articolo 14 sulla inviolabilità del domicilio, l'articolo 15 sulla segretezza della corrispondenza e di ogni altra forma di comunicazione.

In via generale, comunque, il diritto alla riservatezza ha seguito una sorte simile ad altri diritti « nuovi » e ha trovato tutela costituzionale tramite un ancoraggio alla fattispecie aperta rappresentata dall'articolo 2 della Costituzione<sup>(76)</sup>.

Tale diritto, anche diffuso con l'ampio appellativo anglosassone *privacy*, viene descritto come il diritto a tenere segreti aspetti, comportamenti, atti, relativi alla sfera intima della persona, impedendo che tali informazioni vengano divulgate senza l'autorizzazione del soggetto interessato. Oltre all'aspetto « negativo » del diritto, inteso come diritto a non subire intromissioni nella propria sfera privata, la *privacy* ha un aspetto « dinamico », poiché il soggetto ha il potere di controllare la diffusione dei propri dati, scegliendo cosa rendere accessibile a terzi e intervenendo a fronte di comportamenti di turbativa o aggressione<sup>(77)</sup>.

## 1.3 Le indicazioni sovranazionali

A livello sovranazionale, il medesimo diritto è protetto dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle

(74) Cass. civ., sez. III, 3 luglio 2024, n. 18276.

(75) Tanto il primo quanto il secondo aspetto del diritto hanno avuto, nell'elaborazione giurisprudenziale, una rilevante capacità espansiva, evolvendo verso forme di tutela più estese di quelle circoscritte dalle norme di diritto positivo dianzi ricordate. Con riguardo al contenuto positivo del diritto, il crescente riconoscimento sociale della facoltà della persona di apparire in pubblico nella misura in cui abbia interesse a farlo, si è tradotto nel giudizio di meritevolezza di tutela (art. 1322, secondo comma, codice civile) dell'interesse patrimoniale del soggetto allo sfruttamento commerciale della propria immagine verso un corrispettivo, ponendo le basi, da un lato, per la diffusione del contratto atipico di sponsorizzazione (Cass. civ. n. 9880 del 1997; Cass. civ. n. 7083 del 2006; Cass. civ. n. 12801 del 2006; Cass. civ. n. 18218 del 2009); dall'altro lato, per il riconoscimento della risarcibilità del pregiudizio economico rappresentato dalla perdita del corrispettivo dell'utilizzazione della propria immagine a fini pubblicitari (Cass. civ. n. 22513 del 2004; Cass. civ. n. 1875 del 2019), così autorizzandosi la dottrina a ritenere esistente, anche nel nostro ordinamento, la figura, di derivazione americana, del *right of publicity*.

(76) Corte Cost., 5 aprile 1973, n. 38.

(77) Cass. civ., sez. I, 21 agosto 2024, n. 23018.

libertà fondamentali (CEDU) ove, all'articolo 8, paragrafo 1, stabilisce che *«ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza»*, con la precisazione, al successivo paragrafo 2, che *«non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute e della morale, o alla protezione dei diritti e delle libertà altrui»*.

La Corte EDU è, poi, chiamata a controllare che le autorità statuali effettuino un corretto bilanciamento tra gli interessi concorrenti sopra indicati. La nozione di vita privata, elaborata dalla giurisprudenza della Corte di Strasburgo, è ampia, non soggetta ad una definizione esaustiva, che comprende l'integrità fisica e morale della persona e può includere numerosi aspetti dell'identità di un individuo, tra cui spicca proprio il diritto all'immagine. In particolare, la Corte EDU ha evidenziato che il concetto di vita privata si estende ad aspetti relativi all'identità personale, come il nome, la foto o l'integrità fisica e morale di una persona, spiegando che la garanzia offerta dall'articolo 8 CEDU è intesa innanzitutto ad assicurare lo sviluppo, senza ingerenze esterne, della personalità di ciascun individuo nelle sue relazioni con gli altri esseri umani.

Per quanto riguarda le fotografie, la Corte ha affermato che l'immagine di una persona costituisce uno degli attributi principali della sua personalità, poiché rivela le caratteristiche uniche dell'individuo e lo distingue dai suoi pari. Il diritto alla tutela della propria immagine è quindi una delle componenti essenziali dello sviluppo personale. Ciò presuppone principalmente il diritto dell'individuo a controllare l'uso di tale immagine, compreso il diritto di rifiutarne la pubblicazione<sup>(78)</sup>.

Anche l'articolo 7 della Carta dei diritti fondamentali dell'Unione europea (Carta di Nizza) sancisce che *«ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni»*. Il successivo articolo 8, ai commi 1 e 2, della stessa Carta stabilisce, poi, che *«Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge»*.

In una recente pronuncia, poi, la Corte di Giustizia dell'Unione europea (CGUE), affrontando il tema del bilanciamento tra il diritto all'oblio e quello all'informazione (in una fattispecie in cui si trattava di valutare la domanda volta ad ottenere dal gestore di un motore di ricerca la deindicizzazione di alcune immagini riferite a una determinata persona), ha ricordato che l'articolo 7 della Carta di Nizza, relativo al diritto al rispetto della vita privata e familiare, contiene il riferimento a diritti corrispondenti a quelli garantiti dall'articolo 8, paragrafo 1, CEDU, aggiungendo che la protezione dei dati personali svolge un ruolo

(78) Corte EDU, Grande Camera, 7 febbraio 2012, Von Hannover c. Germania, par. 95-96.

fondamentale per l'esercizio del diritto al rispetto della vita privata e familiare, sancito, appunto, dall'articolo 8 CEDU <sup>(79)</sup>.

## 2. Il risarcimento del danno conseguente all'abuso dell'immagine altrui

Passando ad esaminare il tema del risarcimento del danno conseguente all'abuso dell'immagine altrui, con riferimento al danno non patrimoniale conseguente alla lesione di diritti inviolabili della persona, la Corte Suprema di Cassazione ha più volte ritenuto che il danno è risarcibile a condizione che l'interesse leso abbia rilevanza costituzionale; che la lesione dell'interesse sia grave (nel senso che l'offesa superi la soglia minima di tollerabilità imposta dai doveri di solidarietà sociale); che il danno non sia futile (e, cioè, non consista in meri disagi o fastidi) e che, infine, vi sia specifica allegazione del pregiudizio, non potendo assumersi la sussistenza del danno *in re ipsa* <sup>(80)</sup>.

Lo stesso principio è stato enunciato in relazione al danno conseguente alla violazione del diritto all'immagine <sup>(81)</sup>.

Il medesimo orientamento si rinviene con riferimento al danno non patrimoniale, risarcibile ai sensi dell'articolo 15, decreto legislativo 30 giugno 2003, n. 196, noto come recante il Codice in materia di protezione dei dati personali, determinato da una lesione del diritto fondamentale alla protezione dei dati personali, tutelato dagli articoli 2 e 21 della Costituzione. e dall'articolo 8 CEDU, in relazione al quale la Corte Suprema di Cassazione ha evidenziato che il risarcimento non si sottrae alla verifica della «gravità della lesione» e della «serietà del pregiudizio», dovendo essere effettuato il bilanciamento con il principio di solidarietà ex articolo 2 della Costituzione, di cui il principio di tolleranza della lesione minima è intrinseco precipitato, con la conseguenza che determina una lesione ingiustificabile del diritto, non la mera violazione delle prescrizioni poste dall'articolo 11 del decreto legislativo citato, ma solo quella che ne offenda in modo sensibile la sua portata effettiva <sup>(82)</sup>.

In una recente pronuncia, la Corte Suprema di Cassazione, nel ribadire, sempre in tema di illecito trattamento dei dati personali,

(79) Corte di Giustizia della Unione Europea, Grande Camera, 8 dicembre 2022, C-460/20, par. 59. In particolare, secondo la CGUE, occorre attribuire a detto articolo 7 lo stesso significato e la stessa portata di quelli conferiti dall'articolo 8, paragrafo 1, della CEDU, come interpretato dalla giurisprudenza della Corte europea dei diritti dell'uomo. In tale ottica, la CGUE ha evidenziato anch'essa che l'immagine di un individuo è «uno dei principali attributi della sua personalità in quanto esprime la sua originalità e gli permette di distinguersi dalle altre persone. Il diritto della persona alla protezione della sua immagine costituisce una delle condizioni per la sua realizzazione personale e presuppone principalmente il controllo sulla propria immagine da parte di tale persona, che comprende, in particolare, la possibilità per quest'ultima di rifiutarne la diffusione. Ne consegue che, pur se, indubbiamente, la libertà di espressione e d'informazione comprende la pubblicazione di fotografie, la tutela del diritto alla vita privata assume in tale contesto un'importanza particolare, data la capacità delle fotografie di veicolare informazioni particolarmente personali, se non intime, su un individuo o la sua famiglia».

(80) Cass. civ., sez. III, 29 novembre 2023, n. 33276; v. anche Cass. civ., sez. VI-L, 12 novembre 2019, n. 29206.

(81) Cass. civ., sez. III, 12 aprile 2022, n. 11768.

(82) Cass. civ., sez. VI-1, 20 agosto 2020, n. 17383.

l'esclusione del principio del danno *in re ipsa*, ha anche spiegato che la mera violazione delle prescrizioni formali in tema di trattamento del dato può non determinare il danno, ma il risarcimento deve ritenersi dovuto per quella violazione che, concretamente, offenda la portata effettiva del diritto alla riservatezza<sup>(83)</sup>.

Come sopra evidenziato, il diritto alla protezione della propria immagine costituisce un diritto della personalità, che trova fondamento nell'articolo 2 della Costituzione e riconoscimento nell'articolo 8 CEDU, oltre che nell'articolo 7 della Carta di Nizza.

## 2.1. L'accertamento della effettività della lesione

In giurisprudenza si è a lungo discusso sulla questione dell'accertamento della effettività della lesione, richiesta ai fini della risarcibilità del danno.

Diffondere il ritratto fotografico di una persona senza il suo consenso costituisce un illecito, il cui evento lesivo si verifica proprio con il fatto che viene resa pubblica l'immagine della persona interessata, la quale, invece, voleva conservarne la riservatezza.

A differenza dal pregiudizio all'onore o alla reputazione, che si configura come conseguenza della pubblicità dell'immagine<sup>(84)</sup>, in questo caso il pregiudizio è dato proprio dalla pubblicità dell'immagine, che l'interessato voleva mantenere riservata. Tale danno è cagionato dalla condotta lesiva dell'immagine altrui e, come in precedenza evidenziato, deve essere accertato nella sua effettiva esistenza e nella sua serietà. Non può, dunque, ritenersi che l'abuso dell'immagine altrui non abbia provocato alcun danno, in ragione del fatto che, insieme all'immagine, non sia stato pubblicato il nome o le altre generalità della persona interessata, poiché il bene protetto è la riservatezza dell'immagine stessa e non del nome o di altra informazione personale dell'interessato.

L'immagine della persona, come evidenziato dalla Corte EDU e anche dalla Corte di Giustizia dell'Unione europea nelle pronunce sopra menzionate, costituisce in sé un elemento altamente caratterizzante l'identità dell'individuo, che lo rende unico e originale, come tale riconoscibile, in relazione alla quale deve essere rispettata la volontà del titolare che non sia esposta al pubblico, ma riservata alla sfera della vita privata.

Nell'accertamento dell'effettività e serietà della lesione, il giudice di merito è chiamato a esaminare gli elementi in fatto della condotta per valutare la sufficienza, ai fini del ripristino della situazione di diritto, del divieto di utilizzazione dei ritratti fotografici, ovvero la necessità di riparare ad un pregiudizio effettivamente cagionato mediante il risarcimento del danno che sia stato richiesto e provato.

## 2.2. Il criterio risarcitorio del c.d. prezzo del consenso

L'illecita pubblicazione dell'immagine altrui obbliga al risarcimento anche dei danni patrimoniali, che consistono nel pregiudizio

(83) Così Cass. civ., sez. I, 12 maggio 2023, n. 13073.

(84) V., per tali ultime ipotesi, Cass. civ., sez. lav., 8 febbraio 2021, n. 2968; Cass. civ., sez. III, 18 febbraio 2020, n. 4005; Cass. civ., sez. I, 5 agosto 2019, n. 20885.

economico di cui la persona danneggiata abbia risentito per effetto della pubblicazione e di cui abbia fornito la prova.

In ogni caso, qualora non possano essere dimostrate specifiche voci di danno patrimoniale, la parte lesa può far valere il diritto al pagamento di una somma corrispondente al compenso che avrebbe presumibilmente richiesto per concedere il suo consenso alla pubblicazione, determinandosi tale importo in via equitativa, avuto riguardo al vantaggio economico conseguito dall'autore dell'illecita pubblicazione e ad ogni altra circostanza congruente con lo scopo della liquidazione, tenendo conto, in particolare, dei criteri enunciati dall'art. 128, secondo comma, della legge n. 633 del 1941, sulla protezione del diritto di autore<sup>(85)</sup>.

Con sentenza n. 12433 del 2008, la Corte Suprema di Cassazione ha affermato che, fermo restando il diritto al risarcimento del danno per l'indebita pubblicazione dell'immagine, «è indubbio che in molti casi non appare agevole né configurare natura e entità del pregiudizio propriamente economico, né quantificarne l'importo», soprattutto «qualora il soggetto leso non sia persona nota, alla cui immagine possa essere attribuito un valore economico oggettivamente determinabile». Quella pronuncia ha così identificato il criterio risarcitorio del c.d. prezzo del consenso, consistente nel ritrasferire in capo al titolare del diritto quel vantaggio economico del quale l'autore dell'illecito si è indebitamente appropriato. Con la sentenza n. 11353 del 2010, poi, i giudici di legittimità hanno stabilito che l'utilizzo dell'immagine altrui senza il consenso dell'interessato può considerarsi lecita solo ricorrendo una delle ipotesi di cui all'articolo 97 della legge n. 633 del 1941, dovendosi diversamente ritenere tale comportamento fonte di un illecito tale da determinare l'insorgenza del diritto al risarcimento del danno.

Il diritto al risarcimento del danno non fa eccezione rispetto alle regole generali dell'articolo 2043 del codice civile con conseguente onere della prova, a carico del danneggiato, del danno subito e del nesso di causalità tra il comportamento illecito e quel danno<sup>(86)</sup>; tanto in conformità alla consolidata giurisprudenza di legittimità che nega l'esistenza del danno *in re ipsa*<sup>(87)</sup>.

In tema di danno patrimoniale, conseguente a plurime violazioni di legge relative alla pubblicazione di foto della propria vita privata, quand'anche relative a un soggetto molto conosciuto, dall'eventuale rifiuto del soggetto leso di consentire a chicchessia la pubblicazione delle immagini abusivamente utilizzate, non discende affatto l'ab-

(85) Cass. civ. 16 maggio 2008, n. 12433, confermata da Cass. civ. 11 maggio 2010, n. 11353, che, ponendosi il problema della tecnica liquidatoria del danno patrimoniale, in un altro caso di pubblicazione abusiva di fotografie (non autorizzate), ha affermato il principio secondo cui «l'illecita pubblicazione dell'immagine altrui obbliga al risarcimento anche dei danni patrimoniali, che consistono nel pregiudizio economico di cui la persona danneggiata abbia risentito per effetto della predetta pubblicazione e di cui abbia fornito la prova. In ogni caso, qualora non possano essere dimostrate specifiche voci di danno patrimoniale, la parte lesa può far valere il diritto al pagamento di una somma corrispondente al compenso che avrebbe presumibilmente richiesto per concedere il suo consenso alla pubblicazione, determinandosi tale importo in via equitativa, avuto riguardo al vantaggio economico conseguito dall'autore dell'illecita pubblicazione e ad ogni altra circostanza congruente con lo scopo della liquidazione».

(86) Cass. civ., sez. III, 12 aprile 2022, n. 11768.

(87) Cass. civ., sez. I, 23 gennaio 2019, n. 1875.

bandono del diritto, con la conseguente sua caduta in pubblico dominio, in quanto nella gestione del diritto alla propria immagine ben si colloca la facoltà, che si può protrarre per il tempo ritenuto necessario, di non pubblicare determinate fotografie, senza che ciò comporti alcun effetto ablativo e, per altro verso, la stessa gestione del diritto assoluto può comportare la scelta di non sfruttare economicamente i propri dati personali, perché lo sfruttamento può risultare lesivo, in prospettiva, del bene protetto<sup>(88)</sup>.

---

(88) Nei casi in cui il titolare del bene protetto non intenda concedere lo sfruttamento della riproduzione fotografica dei propri dati personali ad altri, non può essere escluso un danno patrimoniale, atteso che anche qualora non possano essere dimostrate specifiche voci di danno patrimonialmente valutabile, la parte lesa, se non può far valere il diritto al pagamento di una somma corrispondente al compenso che avrebbe presumibilmente domandato per concedere il suo consenso alla pubblicazione (che non cade in pubblico dominio), può comunque chiedere una determinazione di tale importo in via equitativa, avuto riguardo alla consistenza del vantaggio economico conseguito dall'autore dell'illecita pubblicazione e ad ogni altra circostanza congruente con lo scopo della liquidazione.

## Parte II LA TUTELA PENALE: LE IPOTESI DI REATO

### 1. Diffusione non consensuale di immagini sessualmente esplicite

#### 1.1 L'origine

Il delitto di diffusione illecita di immagini o video sessualmente espliciti è stato introdotto nel nostro ordinamento in seguito a fenomeni sempre più diffusi e culminati in noti fatti di cronaca.

Ancor prima che tali condotte assumessero rilievo nella dimensione penalistica, il neologismo *revenge porn* era già entrato a far parte del linguaggio di uso corrente, sulla scia di quanto già avvenuto nel mondo anglosassone, in cui l'espressione, dapprima colloquiale e appartenente al linguaggio *slang*, si è diffusa a tal punto da penetrare nel Dizionario di Cambridge, che la definisce come «*private sexual images or films showing a particular person that are put on the internet by a former partner of that person, as an attempt to punish or harm them*».

Tuttavia questo termine non va utilizzato perché contribuisce alla stigmatizzazione del fenomeno poiché, secondo tale terminologia, l'autore è in via esclusiva l'ex partner che, con la finalità di ottenere vendetta, pubblica immagini intime o dal contenuto sessuale, destinate a rimanere private, ritraenti colui/colei che ha posto fine alla relazione sentimentale. In realtà, i casi *Phica.eu*, *Mia Moglie* e *Telegram* dimostrano che la vendetta non è necessariamente un elemento fondante della violenza e che più spesso sono le dinamiche di omosocialità maschile a fomentare questo tipo di fenomeno. Inoltre non si tratta di pornografia ma di materiale sessuale privato.

Secondo le credenze più diffuse gli ingredienti essenziali per la configurazione di un'ipotesi di diffusione non consensuale di immagini intime, come risulta dall'elaborazione semantica della definizione, sono costituiti dalla creazione consensuale di immagini intime o sessuali all'interno di un contesto di coppia, dalla non consensuale pubblicazione delle stesse da parte di uno dei membri della coppia e dalla finalità perseguita dall'ex partner, che pubblica le immagini, solitamente su internet, per vendicarsi a seguito della rottura della relazione sentimentale.

Nel linguaggio comune, tuttavia, i confini della definizione si sono dimostrati estremamente fluidi, nel senso che l'espressione *revenge porn* rimane limitata per indicare tutte le varie possibili forme di diffusione non consensuale di immagini sessualmente connotate<sup>(89)</sup>.

Come messo in risalto da alcuni esegeti, il Parlamento italiano ha tentato di fronteggiare il fenomeno, ormai dilagante anche in Italia, attraverso un *iter* che, sempre sulla scia di fatti di cronaca, ha portato alla introduzione nel codice penale dell'articolo 612-ter, mediante la presentazione di un emendamento al disegno di legge governativo Atto

(89) In questa prospettiva, quindi, come si è osservato da una parte della dottrina, «*revenge porn*» è al tempo stesso un po' metonimia e un po' sineddoche: da un lato, infatti, si pone l'accento sulla causa, ossia la vendetta, anziché sull'effetto, cioè il danno subito dalla vittima, e, dall'altro, si utilizza una terminologia che indica uno specifico fenomeno per richiamare situazioni diversificate tra loro, anche se accomunate dalla divulgazione non consensuale di immagini sessuali.

Camera n. 1455, poi approvato definitivamente e divenuto legge 19 luglio 2019, n. 69 (c.d. « Codice Rosso »), inserendo, quindi, la nuova norma all'interno di un più ampio pacchetto legislativo, dedicato alla tutela delle vittime di violenza domestica e di genere, anziché, come auspicato da taluni, nell'ambito di un più meditato inserimento del nuovo reato in un nuovo e apposito titolo del codice sui delitti contro la riservatezza sessuale.

A fronte della portata semantica originaria dell'espressione tratta dallo *slang* inglese — consistente, come detto, nella pubblicazione, da parte di uno dei due membri di una coppia, di immagini o video dell'ex partner, già consensualmente acquisiti e caratterizzati da un contenuto intimo e sessualmente esplicito, per vendicarsi a seguito della rottura della relazione sentimentale —, la dottrina penalistica angloamericana, spostando l'accento dalle finalità vendicative del soggetto agente, ha puntualizzato il baricentro del fenomeno lesivo nella totale assenza del consenso alla divulgazione dei contenuti espliciti, la cui creazione e la cui permanenza si è — erroneamente, dal lato della vittima — supposta nell'ambito di una sfera privata, di carattere profondamente intimo<sup>(90)</sup>.

In ogni caso, come evidenziato dalle prime analisi della dottrina, la portata comunicativa dell'espressione *revenge porn* ha trovato fortuna nel linguaggio mediatico e comune, divenendo, anche nel nostro Paese, una sorta di *catch-all phrase* utilizzata per indicare tutte le diverse forme di diffusione non consensuale di immagini aventi un contenuto sessuale.

## 1.2 Gli elementi costitutivi

L'articolo 612-ter del codice penale sanziona, al primo comma, il responsabile della divulgazione, che può essere posta in essere mediante plurime condotte, e, al secondo comma, con la stessa pena, i « secondi distributori » delle immagini sessualmente esplicite.

La norma non solo richiede l'assenza di consenso, ma anche che le immagini o i video siano « destinati a rimanere privati », come se, si è osservato in dottrina, ancor prima dell'assenza di consenso alla divulgazione, vi sia la rottura di un *pactum fiduciae* tra due individui, presumibilmente legati da una relazione, tale da aver impresso una precisa destinazione ai contenuti, poi disattesa da uno dei due.

Si è anche osservato che nell'*iter* parlamentare non figura alcuna relazione o commento a tale inciso, per cui può ritenersi, verosimilmente, che lo stesso costituisca una sorta di traslitterazione, da parte del legislatore italiano, di altre esperienze legislative, senza considerare come, invece, il fenomeno, dal punto di vista casistico, in moltissimi casi esorbita del tutto da un contesto di coppia, potendosi, invece, inquadrare anche in rapporti del tutto occasionali.

Nell'ottica dell'interprete non è possibile prescindere dalla valenza e dal rango elevato dei beni protetti dalla norma in esame, ossia i valori dell'intimità e della *privacy*, quale diritto a controllare l'esposizione del proprio corpo e della propria sessualità, a prescindere dal contesto e dalle finalità con le quali avviene la divulgazione.

Ciò che rileva, quindi, è il diritto ad autodeterminarsi in ordine alla propria sfera sessuale, mediante un consenso libero ed effettivo, la cui

(90) Cass. pen., sez. V, 1° marzo 2024, n. 24379.

mananza assume un rilievo decisivo nell'individuazione della fattispecie. Il che induce a ritenere, anche alla luce delle considerazioni svolte in precedenza in riferimento all'evoluzione ermeneutica delle condotte e alla latitudine del sintagma *revenge porn*, che la condotta incriminata sia più ampia di quella realizzata unicamente nell'ambito di un pregresso rapporto sentimentale, nel cui contesto si sia verificato un utilizzo diverso del materiale originariamente destinato a rimanere circoscritto e riservato.

In tal senso, infatti, la rubrica della norma delinea la rilevanza penale della diffusione illecita di immagini e video sessualmente espliciti, senza alcun riferimento a uno specifico contesto di pregressa relazione sentimentale. Tale contesto, non a caso, fonda la circostanza aggravante delineata al terzo comma della norma richiamata, il che rende evidente come il fulcro della incriminazione sia costituito dalla totale assenza di consenso della persona offesa alla divulgazione dei materiali a contenuto sessuale esplicito, a prescindere da qualsiasi intento di rivalsa dell'autore del reato e dall'inquadramento della condotta in un precedente legame sentimentale, connotazioni del tutto assenti dall'impianto normativo, anche se utili alla ricostruzione della genesi della emersione delle condotte penalmente rilevanti.

Ciò nondimeno, dalla formulazione normativa emerge chiaramente come il profilo del consenso – la cui assenza alla diffusione del materiale a contenuto esplicitamente sessuale costituisce elemento costitutivo della fattispecie – sia logicamente presupposto al momento della formazione del materiale stesso; la norma, cioè, presuppone la consapevolezza e il consenso alla produzione di tale materiale, da parte della persona offesa, essendo il materiale, nella fase « genetica » destinato a rimanere confinato nell'ambito di una sfera privata, sia essa di coppia stabile o meno.

La rilevanza penale delle condotte descritte nelle fattispecie incriminatrici, quindi, risiede nella fuoriuscita del materiale, connotato da contenuto sessuale esplicito, dall'originario perimetro relazionale privato, per cui all'assenza di consenso come requisito di tipicità si accompagna anche la caratterizzazione « privata » della destinazione dell'oggetto materiale del reato, ossia il materiale sessualmente esplicito.

I due requisiti – la destinazione privata e la mancanza di consenso – devono sussistere entrambi contemporaneamente e non possono operare in alternativa tra loro.

La divulgazione di cui al primo comma dell'articolo 612-ter del codice penale, quindi, ha come retroterra – espresso dall'inciso « *destinati a rimanere privati* » – e, quindi, come presupposto la formazione intra-relazionale del materiale a contenuto sessualmente esplicito, ossia la formazione del materiale a opera degli stessi soggetti che vi sono rappresentati.

Conseguentemente, e altrettanto inequivocabilmente, emerge, dalla formulazione testuale del primo comma dell'articolo 612-ter, che l'autore di una delle condotte di diffusione del materiale a contenuto sessualmente esplicito non possa che essere il soggetto che ha realizzato il materiale stesso, oppure colui che lo ha sottratto: « *Salvo che il fatto costituisca più grave reato, chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto*

*sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate ... ».*

In altri termini: sebbene non risulti necessario che le immagini a contenuto sessualmente esplicito siano state realizzate in un contesto relazionale sentimentale stabile, successivamente interrotto, con correlata volontà di rivalsa da parte del soggetto agente, ciò nondimeno l'autore della condotta deve essere colui che aveva in precedenza realizzato il detto materiale o che se ne era impossessato sottraendolo.

La formulazione della norma — «... *chi, avendo ricevuto o comunque acquisito le immagini o i video di cui al primo comma ...* »— rende evidente come il legislatore abbia individuato il « diffusore secondario » del materiale in colui che riceva il materiale dall'autore dello stesso, ossia da chi, ai sensi del primo comma, aveva realizzato il materiale stesso in un contesto relazionale con la persona offesa, che aveva consentito alla produzione delle immagini o dei video in funzione esclusivamente privata.

### **1.3 La nozione di « contenuti sessualmente espliciti »**

La nozione di « contenuti sessualmente espliciti » non può essere limitata soltanto alle immagini o ai video che ritraggano organi genitali ovvero atti sessuali veri e propri.

Il testo normativo non pone esplicite riserve in tal senso, né l'interpretazione giurisprudenziale mostra accenti contrari.

La locuzione normativa « a contenuto sessualmente esplicito » non rimanda evidentemente e necessariamente alla diffusione di video o immagini di un organo proprio dell'apparato sessuale-riproduttivo in senso medico-scientifico, né tantomeno allude solo a un atto sessuale vero e proprio (sulla cui nozione, complessa, molto ci si interroga ai fini dell'integrazione delle diverse fattispecie penali nelle quali essa viene inserita), essendo evidente che la sessualità di una persona, vittima del reato, può essere evocata in maniera manifesta anche soltanto attraverso la proposizione di parti del suo corpo « erogene » diverse dagli organi genitali, eppure capaci di richiamare, per il contesto e le condizioni concrete nelle quali vengono ritratte, l'istinto sessuale. Tali « zone erogene » possono essere il seno e i glutei, ancor più se nudi ovvero in condizioni di contesto che richiamino il sesso. Sicché, qualora la diffusione avvenga senza il consenso della persona offesa, si stabilizzerà una violazione della libertà di autodeterminazione della sua sfera sessuale complessivamente intesa, rilevante ai sensi del secondo comma dell'articolo 612-ter se accompagnata dal dolo specifico di recare nocumento alla persona le cui immagini (o video) vengano diffusi.

Inoltre, seguendo le declinazioni interpretative della disciplina penale della pornografia minorile, nella quale egualmente viene in gioco il tema della sessualità e del significato sessuale d'immagini, si è conferito rilievo sessuale alla nudità in quanto tale <sup>(91)</sup> ovvero anche a movimenti e atteggiamenti, ancorché inconsapevoli o involontari <sup>(92)</sup>, per cui, ai fini della configurabilità del delitto di pornografia minorile, il

(91) Cass. pen., sez. III, 1° dicembre 2017, n. 39685.

(92) Cass. pen., sez. III, 10 giugno 2015, n. 42964.

carattere pedopornografico del « materiale prodotto » non presuppone necessariamente un'interazione consapevole fra l'autore della condotta e il minore presentato, ben potendo essere individuato nella rappresentazione di movimenti in cui i minori assumono posizioni che si concretizzano in atteggiamenti lascivi ed eroticamente eccitanti, seppur assunti involontariamente e inconsapevolmente.

Sempre in tema di pornografia minorile, è stato precisato che il riferimento alla « *rappresentazione degli organi sessuali di un minore di anni diciotto* » di cui all'ultimo comma dell'articolo 600-ter del codice penale, ricomprende non solo gli organi genitali, ma anche altre zone erogene, come il seno e i glutei<sup>(93)</sup>.

Il reato di diffusione illecita di contenuti sessualmente espliciti, pertanto, può avere per oggetto immagini o video che ritraggano atti sessuali ovvero organi genitali ovvero anche altre parti erogene del corpo umano, come i seni o i glutei, nudi o in condizioni e contesto tali da evocare la sessualità<sup>(94)</sup>.

Il contenuto « sessualmente esplicito », al quale fa riferimento l'articolo 612-ter del codice penale, dunque, non può identificarsi nella riproduzione di rapporti sessuali (o di autoerotismo) o ancora di organi propri dell'apparato sessuale-riproduttivo in senso scientifico<sup>(95)</sup>. La sessualità di una persona, vittima del reato, può essere evocata in maniera manifesta anche soltanto attraverso la proposizione di parti del suo corpo « erogene » diverse dagli organi genitali, eppure capaci di richiamare, per il contesto e le condizioni concrete nelle quali vengono ritratte, l'istinto sessuale<sup>(96)</sup>.

Lucia Bainotti, Assistant Professor in Digital and Visual Media Analysis presso il Dipartimento di Media Studies dell'Università di Amsterdam<sup>(97)</sup>, ha suggerito di ampliare l'ambito di applicazione della norma includendo « *non solo materiali intimi, materiali sessualmente espliciti, ma anche materiali intimi non di natura sessuale e altre forme di abusi digitali, questo proprio perché molto spesso vediamo che i materiali condivisi on line sono più semplicemente immagini intime e non necessariamente sessualmente esplicite. Abbiamo bisogno di tutela rispetto a questa dimensione* ».

#### 1.4 Il consenso a farsi riprendere non esclude il reato

Quello che caratterizza la condotta illecita è che la persona offesa, della quale viene violata la sfera più intima che costituisce il bene protetto dalla norma incriminatrice, non abbia prestato consenso alla divulgazione delle proprie immagini sessuali a soggetti differenti da quelli con i quali abbia realizzato le immagini o il video a contenuto sessualmente esplicito.

In altri termini, non assume alcuna rilevanza, ai fini della configurabilità del delitto, la circostanza che la vittima abbia prestato il suo

(93) Cass. pen., sez. III, 8 gennaio 2020, n. 9354; vedi anche Cass. pen., sez. III, 15 novembre 2005, n. 549.

(94) Cass. pen., sez. I, 28 marzo 2024, n. 33230.

(95) Così Cass. pen., sez. V, 22 febbraio 2023, n. 14927.

(96) Così Cass. pen., sez. V, 29 marzo 2023, n. 32602, che ha confermato la condanna per *revenge porn* inflitta ad un uomo che aveva diffuso *on line* video e foto che ritraevano una persona semplicemente in biancheria intima e non impegnata in espliciti atti sessuali.

(97) Audizione del 17 novembre 2025.

consenso a farsi ritrarre o riprendere nel video oggetto di successiva divulgazione, purché il consenso, beninteso, non riguardi anche detta divulgazione<sup>(98)</sup>.

In sostanza, l'articolo 612-ter del codice penale sanziona due fattispecie identiche per condotta (inviare, consegnare, cedere, pubblicare o diffondere senza il consenso delle persone rappresentate) e oggetto materiale (immagini o video a contenuto sessualmente esplicito destinati a rimanere privati), ma diverse per presupposto (nel primo caso, aver realizzato o sottratto, nel secondo caso, aver ricevuto o comunque acquisito le immagini o i video) e per fine (irrilevante, nel primo caso, trovandoci quindi in presenza di fattispecie a dolo generico; essenziale, nel secondo, il « fine di recare nocumento » alla vittima costituendo l'oggetto del dolo specifico).

La norma sanziona, così, condotte di carattere plurioffensivo che non comportano solo la lesione dell'onore e della reputazione della vittima, come, peraltro, si evince dalla collocazione sistematica del delitto, subito dopo le fattispecie di violenza privata, minaccia e atti persecutori, palesando un'oggettività giuridica che ricomprende l'area della libertà di autodeterminazione, anche (ma non solo) sessuale, in una tutela della sfera intima della persona che si è reso necessario rafforzare anche a fronte della maggiore offensività ai beni protetti derivante dal massiccio utilizzo di mezzi informatici.

In conclusione, per l'integrazione del delitto non assume alcuna rilevanza il consenso della vittima a farsi ritrarre nel video a contenuto sessualmente esplicito, poiché ciò che è determinante è il non aver prestato consenso alla divulgazione dello stesso ad altri soggetti.

#### 1.4.1 I contenuti su « *OnlyFans* »

Il delitto di diffusione illecita di immagini o video sessualmente espliciti<sup>(99)</sup> è integrato anche dalla condotta di chi, avendo ricevuto o comunque acquisito materiale visivo pubblicato sul sito *web OnlyFans*<sup>(100)</sup>, lo trasmette a terzi senza il consenso della persona ritratta, in quanto il consenso espresso da quest'ultima al momento della condivisione (a pagamento) è circoscritto alla facoltà di visualizzazione del solo destinatario del contenuto<sup>(101)</sup>.

Per la giurisprudenza, commette il delitto di *revenge porn* chi, avendo ricevuto, o comunque acquisito, materiale visivo pubblicato su un sito *web* con accesso limitato ai soli iscritti, lo trasmetta a terzi senza il consenso della persona ritratta, in quanto tale facoltà, in virtù del consenso espresso da quest'ultima al momento dell'apertura dell'*account*, è circoscritta ai soli appartenenti alla comunità virtuale a cui il

(98) Cass. pen., sez. V, 23 febbraio 2024, n. 19201; Cass. pen., sez. V, 22 febbraio 2023, n. 14927.

(99) Il reato è inserito tra quelli a tutela della libertà morale individuale e si rivolge alla sfera d'intimità personale e della *privacy*, intesa quale diritto a controllare l'esposizione del proprio corpo e della propria sessualità, in un'ottica di autodeterminazione della sfera sessuale individuale. Cass. pen., sez. I, 28 marzo 2024, n. 33230 cit..

(100) *OnlyFans* è una piattaforma *social* basata su un modello di abbonamento, dove i *creator* possono condividere contenuti di ogni tipo – dai più creativi a quelli espliciti – e guadagnare grazie a sottoscrizioni, donazioni e contenuti *pay-per-view*. I *creator*, quindi, possono caricare contenuti esclusivi per i propri *follower*, che possono guardare solo previo pagamento.

(101) Cass. pen., sez. V, 12 giugno 2025, n. 30169.

materiale era stato originariamente inviato e unicamente all'interno di essa<sup>(102)</sup>.

### 1.5 Il rapporto con il reato di *stalking*

Il *revenge porn* differisce dallo *stalking*, in primo luogo, per ciò che riguarda le condotte incriminate, costituite nell'articolo 612-*bis* del codice penale da comportamenti minacciosi o molesti e nell'articolo 612-*ter* del codice penale nella diffusione di immagini a contenuto sessualmente esplicito (in assenza del requisito della violenza o della minaccia).

In secondo luogo, sono diversi gli eventi ravvisabili, per lo *stalking*, nell'induzione nella vittima di stati di ansia, paura o timore per l'incolumità propria o di congiunti, ovvero nella costrizione della persona offesa all'alterazione delle proprie abitudini di vita; eventi all'evidenza non richiesti per la configurabilità del *revenge porn*.

Sono altresì differenti i beni giuridici tutelati.

Nonostante i due reati siano collocati nel codice penale tra quelli che ledono la libertà morale, l'articolo 612-*ter* si atteggia quale reato plurioffensivo, incidendo anche sulla *privacy* della persona offesa (come impone di ritenere l'inciso « *destinati a rimanere privati* »), nonché sulla sfera sessuale, a causa del carattere « *sessualmente esplicito dei materiali diffusi* »<sup>(103)</sup>.

Stante, dunque, l'obiettivo diversità tra il fatto idoneo a integrare ciascuno dei due delitti (dei quali, peraltro, il primo ha natura abituale mentre l'altro è reato istantaneo), non può assumere rilievo il riferimento alla clausola di riserva contenuta nel primo comma dell'articolo 612-*ter* (« *salvo che il fatto costituisca più grave reato* », presente anche nel reato di *stalking*), che sembra piuttosto evocare altre fattispecie incriminatrici (ad esempio il reato di estorsione). Infine, l'innalzamento della pena per il reato di cui all'articolo 612-*bis* non è in alcun modo riconducibile all'intenzione del legislatore di ricomprenservi le condotte di cui all'articolo 612-*ter*, rispondendo a scelte di politica criminale affatto differenti.

### 1.6 Le criticità dei c.d. *shame crimes*

Come rappresentato da Matteo Flora, Presidente dell'associazione PermessoNegato, nel corso della sua audizione<sup>(104)</sup>, in relazione al reato di *revenge porn* si registra un consistente « sommerso ».

Nel periodo 2023-2024, sono state sporte poco più di 500 denunce, nell'83% dei casi da parte di donne. I numeri ufficiali non descrivono la realtà: descrivono solo quella frazione di vittime che ha avuto la forza di superare la vergogna e il timore di non essere credute o, peggio ancora, di essere ricolpevolizzate.

(102) Cass. pen., sez. V, 6 giugno 2025, n. 25516 e, prima ancora, Cass. pen., sez. V, 5 marzo 2024, n. 25516.

(103) Dirimente, quanto all'esclusione dell'ipotesi del reato complesso, è la considerazione che, affinché si realizzi tale fattispecie, il fatto deve essere previsto dalla norma incriminatrice, che si assume configurare un reato complesso, quale elemento necessario della relativa fattispecie astratta, non essendo rilevante l'eventuale sua ricorrenza, nel caso concreto, quale occasionale modalità esecutiva della condotta.

(104) Audizione del 10 novembre 2025.

Parliamo di *shame crimes*, di crimini di vergogna<sup>(105)</sup>.

L'audito ha affermato che, in base ai dati in suo possesso, meno della metà delle vittime sporge denuncia: «*Per capire il fenomeno dobbiamo guardare il sommerso: noi lo abbiamo fatto con un'indagine demoscopica, con oltre 2 mila interviste in Italia, disponibile on line, che ha rivelato una realtà un po' diversa, più in linea con altre nazioni. In proiezione, sono circa 2 milioni gli italiani vittime di revenge porn, 14 milioni gli italiani che hanno visto le immagini (e lì farò una riflessione diversa) e 5 milioni gli italiani che conoscono personalmente una vittima. Il dato più grave, in realtà, è la reiterazione. La violenza digitale prospera dalla ricondivisione. Il 5 per cento degli italiani ammette di aver ricondiviso contenuti intimi di altri e quando abbiamo chiesto loro se lo rifarebbero l'84 per cento ha risposto "sì". Perché? Perché non c'è la percezione del reato, non c'è rimorso, perché è normalizzato, come dicono quelli bravi. Per due su tre è un gioco, uno scherzo; per uno su quattro la deumanizzazione è proprio totale ("tanto non la conosco"); il 17 per cento degli italiani ancora oggi è convinto che la condotta di condivisione senza il consenso non costituisca reato. Non solo, tra l'altro, un crimine di genere, ma più un crimine di potere*».

In relazione al «*NCII*» (*Non-Consensual Intimate Image*), la condivisione non consensuale di immagini, la normalizzazione della diffusione ha conseguenze drammatiche.

La prima criticità è linguistica e psicologica.

Quella che noi chiamiamo «*vergogna*» o «*imbarazzo*» ha un nome specifico: trauma. L'impatto è assimilabile – rilevano gli psicologi – a un disturbo da stress post-traumatico ma, mentre l'aggressione fisica ha un inizio e una fine, la violenza digitale è un trauma perpetuo.

Il materiale può riemergere in qualunque momento. È un *restimulation loop*<sup>(106)</sup>, un *loop* di ri-stimolazione senza fine, che genera iper vigilanza cronica.

### 1.6.1 I c.d. superdiffusori

Il fenomeno del *revenge porn* in Italia, a differenza di quanto accaduto in altre parti del mondo, è esploso perché alimentato dai c.d. *superspreader*<sup>(107)</sup>.

I superdiffusori sono agenti, tecnologie o meccanismi sociali che accelerano esponenzialmente il danno prodotto dalla diffusione di

(105) *Silvia Semenzin*, ricercatrice in sociologia digitale presso l'Università Oberta de Catalunya e membro della ong AI Forensics, nel corso della audizione del 16 ottobre 2025, ha chiarito che, in tema di diffusione non consensuale di materiale intimo, i dati ci raccontano che si tratta di un fenomeno che impatta principalmente sulle donne. In inglese si preferisce utilizzare l'espressione *image-based sexual abuse*, che racconta di un abuso sessuale o di una violenza sessuale basata sull'immagine e sulla condivisione dell'immagine. In italiano non abbiamo una traduzione, quindi è bene continuare a utilizzare almeno l'espressione «*diffusione non consensuale di materiale intimo*». Il 90 per cento delle vittime di condivisione non consensuale è una donna e le conseguenze sono terribili, perché oltre il 51 per cento delle vittime pensa al suicidio come forma di uscita da questo tipo di violenza, per colpa della «*vergogna che le donne sentono di fronte alla violazione della loro intimità e della loro privacy e la disperazione di non sapere come uscire da quella violenza perché sono troppi gli occhi che ci hanno viste*».

(106) Con il termine «*restimulation loop*» si fa riferimento all'atto o al processo di riattivazione di un ricordo del passato dovuto a circostanze simili che si vivono nel presente.

(107) In medicina, il termine indica quegli individui che contribuiscono in modo sproporzionato alla trasmissione di un patogeno.

immagini o video, reali o artefatti, lesivi della reputazione di una persona, soprattutto le piattaforme digitali ancora non coperte da DSA come *Telegram* o i siti web minori come *Phica.eu*.

Oggi non serve più rubare una foto intima. Basta una foto pubblica, presa da un *social* qualunque o da un articolo di giornale o dal profilo della persona per alimentare un'applicazione che spoglia la persona. È una figura tutta nuova, è una sessualizzazione forzata, una violenza psicologica nuova che permette a chiunque di diventare un carnefice. È semplice, tra l'altro, come semplice è l'uso di queste tecnologie che sono alla portata di tutti.

Poi ci sono — ha proseguito *Matteo Flora* nel corso della sua audizione — «*i superdiffusori di distribuzione, le piattaforme "porto franco", le piattaforme "canaglia", come le chiamiamo noi, come Telegram. Sono piattaforme che, trincerandosi dietro policy di non intervento sui contenuti e garantendo più o meno un anonimato, agiscono come una sorta di paradiso dei criminali*».

Un altro superdiffusore è forse il più dannoso perché agisce in buona fede: il giornalismo imprudente. I *media*, i giornalisti, i *creator*, anche nel lodevole tentativo di denunciare un fenomeno, nominano i gruppi e le *chat* dove è avvenuta la pubblicazione o lo scambio del materiale pubblicizzandoli involontariamente<sup>(108)</sup>.

La notizia, nel tentativo di raccontare il fenomeno, lo amplifica, innescando poi una ri-vittimizzazione di massa, perché le persone che sono presenti all'interno di quel gruppo diventano maggiormente esposte alla curiosità altrui. Oltretutto, questo rinforza la normalizzazione, quello che gli esperti chiamano effetto *bandwagon*, effetto carrozzone<sup>(109)</sup>. Il fatto che lo facciano già migliaia di persone, in qualche modo «diluisce» la responsabilità individuale. Il singolo individuo percepisce il messaggio secondo il quale visto che già tanti altri lo stanno facendo può farlo anche lui. Si crea così una pratica sociale, una consuetudine, percepita come lecita.

### 1.6.2 I rimedi

Dalle numerose audizioni e dai documenti acquisiti è possibile evincere una serie di suggerimenti, correttivi al sistema — non solo penale — attuale.

Per contenere il fenomeno della diffusione illecita di immagini o video, reali o creati dall'intelligenza artificiale generativa, dal contenuto sessualmente esplicito è necessario procedere alla formazione dei *contact point*, con l'istituzione di protocolli, l'introduzione di una

(108) Matteo Flora ha raccontato di aver «*monitorato decine di episodi in cui subito dopo un servizio televisivo, un articolo di giornale, il numero degli iscritti a quei canali esplode. C'è un gruppo specifico che dopo un passaggio in televisione è passato da 30.000 membri a 260.000 utenti in meno di dieci giorni, mentre era più o meno costante nel tempo*».

(109) L'effetto carrozzone o effetto *bandwagon* (in inglese *bandwagon effect*) è il fenomeno secondo cui le persone spesso compiono alcuni atti o credono in alcune cose solo perché la maggioranza della gente crede o fa quelle stesse cose. Ci si riferisce spesso in senso dispregiativo a questo effetto chiamandolo «*istinto del gregge*», in particolare riferendosi agli adolescenti. Si può dunque dire che c'è una tendenza nella gente a seguire la folla. L'effetto carrozzone è alla base del successo di quelle argomentazioni basate esclusivamente su opinioni molto diffuse (*argumentum ad populum*). In senso letterale il termine inglese *bandwagon* indica il carro che trasporta la banda musicale in una parata.

formazione obbligatoria per le Forze dell'ordine, su due livelli: la gestione tecnica, perché tante volte non è vero che le piattaforme non rimuovono (ne è la prova il fatto che ad esempio il Garante per la protezione dei dati personali riesce a rimuoverle con un'operazione amministrativa); la gestione psicologica, spiegando come deve essere accolta una vittima in trauma perpetuo.

Occorre una formazione anche per fermare la pubblicità involontaria ricorrendo, per esempio, a un patto di responsabilità con l'Ordine dei giornalisti, per contenere la pratica, non di segnalare la notizia, ma di nominare i gruppi illeciti. Sono centinaia i casi di articoli che dicono come si trova sulla piattaforma X il gruppo X. L'indicazione del nome del gruppo ri-vittimizza generando una forma di vittimizzazione secondaria tra le più gravi in assoluto.

Ci sono poi criticità legislative che rischiano di vanificare gli effetti del potente impianto che ruota intorno al c.d. Codice Rosso.

L'attuale formulazione dell'articolo 612-ter del codice penale punisce chi diffonde e ri-diffonde, ma tace completamente su un attore, anzi forse sull'attore chiave, il fruitore. Chi si limita a ricevere e guardare, a beneficiare del materiale di un gruppo senza compiere azioni di inoltro non commette alcun reato. Non è un dettaglio tecnico, è il motore culturale dell'intero fenomeno. È il vuoto normativo che crea quella zona franca dei « fratelli di godimento ». Il ri-diffusore agisce e ri-diffonde perché sa di avere un pubblico, un mercato, una platea, che « consuma » il materiale senza rischiare nulla.

Vi è poi una seconda lacuna, non meno grave, l'assenza di una riflessione su chi realizza il contenuto. È evidente che il vero invitato di pietra non è solo il fruitore, ma anche colui che consapevolmente o meno produce quel materiale destinato a circolare: oggi chi registra un video intimo, magari in un contesto privato e consensuale e poi lo lascia involontariamente finire nelle mani di chi diffonde, non è punibile. Eppure, in un'ottica di prevenzione e di reale repressione del fenomeno, anche questo anello della catena merita una considerazione dal punto di vista normativo, perché la creazione del contenuto è il primo atto, quello fondamentale, perché rende possibile poi la diffusione del contenuto e della violenza che ne consegue.

Questi *vulnus* creano un paradosso che è insostenibile perché, a differenza di quanto prevedono altri articoli, quali quelli che si occupano di diffusione di materiale pedopornografico (articolo 600-quater del codice penale), dove anche la semplice detenzione integra un reato, perché la visione stessa reitera l'abuso, nel caso della pornografia non consensuale è invece lecita. Lo Stato – ha concluso *Matteo Flora* – ci sta dicendo nei fatti che guardare non è parte del problema. Eppure, è proprio quella parte che alimenta l'offerta.

*Chiara Gius*, coordinatrice nazionale del progetto Prin 2022 « rappresentazioni sociali della cyberviolenza contro donne e ragazze » e ricercatrice presso l'Università di Bologna<sup>(110)</sup>, dopo aver rilevato che la condivisione non consensuale di immagini intime è la pratica più facilmente nominata, perché visibile e mediatizzata, ha osservato che questa centralità rischia di oscurare altre forme meno evidenti, ma altrettanto pervasive, come la sorveglianza digitale nelle relazioni di

(110) Audizione del 20 ottobre 2025.

coppia. Sul piano delle politiche pubbliche e dei servizi questa parzialità di comprensione si traduce in risposte frammentate: da un lato approcci securitari centrati sulla repressione; dall'altro strategie individualizzate che spostano la responsabilità sulle vittime (« non condividere », « stai attenta »), piuttosto che sul contesto tecnologico e sociale che rende possibile certi comportamenti.

**DIFFUSIONE NON CONSENSUALE DI MATERIALE INTIMO**

(IMAGE-BASED SEXUAL ABUSE)

- Il 90% delle vittime di condivisione non consensuale di materiale intimo è una donna (UNESCO, 2023; UN Women, 2023)
- Il 51% delle vittime ha avuto pensieri suicidari (European Institute for Gender Equality, 2019)
- Il 96% dei deepfake che vengono prodotti online sono di natura pornografica (DeepTrace Labs, 2023).
- Il 99% delle vittime di deepfake sessuali sono donne (Home Security Heroes, 2023)



*Slide n. 4 proiettata durante l'audizione del 16 ottobre 2025 di Silvia Semenzin, ricercatrice in sociologia digitale presso l'Università Oberta de Catalunya e membro della ong AI Forensics.*

## 2. Il delitto di diffusione di riprese e registrazioni fraudolente

### 2.1 Gli elementi costitutivi

Il delitto di diffusione di riprese e registrazioni fraudolente è stato introdotto in attuazione della legge delega del 23 giugno 2017, n. 103, intervenuta a seguito di un lungo dibattito critico, generato soprattutto dalla diffusione da parte dei *mass media* dei contenuti delle intercettazioni e dalla lesione del diritto alla riservatezza non solo dei soggetti diretti destinatari dell'intercettazione, ma anche dei soggetti esterni e coinvolti in quanto semplici interlocutori del soggetto-bersaglio.

Il reato intende reprimere comportamenti che violano la riservatezza degli individui (e, contestualmente, la loro reputazione e immagine) tramite la diffusione di materiale raccolto fraudolentemente, al fine di danneggiare i beni giuridici menzionati; con tale innesto, si sono volute colmare lacune emerse nel sistema penale riguardo alla tutela della riservatezza, colpita da aggressioni poste in essere mediante l'impiego di sistemi captativi a carattere tecnologico.

L'articolo 617-septies del codice penale punisce « *chiunque, al fine di recare danno all'altrui reputazione o immagine, diffonde con qualsiasi mezzo riprese audio o video, compiute fraudolentemente, di incontri privati o registrazioni, pur esse fraudolente, di conversazioni, anche telefoniche o telematiche, svolte in sua presenza o con la sua partecipazione* ».

L'inserimento della disposizione nel Libro Secondo (Dei delitti in particolare), Titolo dodicesimo (Dei delitti contro la persona), Capo Terzo (Dei delitti contro la libertà individuale), Sezione Quinta (Dei delitti contro l'inviolabilità dei segreti) del codice penale fornisce indicazioni sul bene giuridico che si intende tutelare: la norma affonda le proprie radici nell'articolo 15 della Costituzione, che tutela la libertà e la segretezza della corrispondenza e di ogni forma di comunicazione, ma anche nell'articolo 21 della Costituzione posto a presidio del diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione.

La tutela della libertà e segretezza delle conversazioni e comunicazioni passa naturalmente anche dalla inviolabilità del domicilio (articolo 14 della Costituzione), dal momento che, con la norma, non si può garantire tutela alla libertà di espressione e manifestazione del pensiero (quale che sia la forma assunta) avvenuta in un contesto e in luogo pubblico per volontà delle parti o per le specifiche modalità con cui la comunicazione/conversazione viene concretamente posta in essere.

Si può cogliere, dunque, la *ratio* della norma incriminatrice, non soltanto nella libertà e segretezza delle conversazioni o comunicazioni, ma anche nella tutela dell'onore e della reputazione degli interlocutori della conversazione, di qualsiasi genere, che avvenga in privato, i cui contenuti sono e devono intendersi destinati a rimanere tra i presenti (i quali hanno diritto a non vedere carpite con l'inganno parole o esternazioni di qualsivoglia genere e a vederle diffuse nell'etere), sempreché non sussista espresso consenso alla divulgazione.

In questo senso, si può affermare che la inviolabilità e la segretezza delle comunicazioni o conversazioni sono protette dalle ingerenze esterne o dalla arbitraria e non autorizzata diffusione *extra praesentes*, non soltanto perché viene in tal modo garantita la libera esplicazione e manifestazione del pensiero, ma anche per evitare che una indebita circolazione dei contenuti di conversazioni o comunicazioni private possa ledere la reputazione e l'onore del soggetto passivo<sup>(111)</sup>.

(111) Giova richiamare un passo della Relazione illustrativa trasmessa al Parlamento, la quale chiarisce che: « *la norma punisce colui che diffonde il contenuto di incontri o conversazioni riservate, registrate con mezzi insidiosi, (microfoni o telecamere nascoste), e quindi fraudolentemente, allo scopo di recare nocumento all'altrui reputazione. Sul piano empirico, la società della comunicazione di massa registra il frequente ricorso a simili stratagemmi, posti scientemente in essere con lo scopo della successiva divulgazione. Si tratta di condotte agevolate dalla diffusione, anche tra privati, di mezzi tecnologici del tutto idonei all'ampia e immediata divulgazione di contenuti comunicativi carpitati senza l'altrui consenso (si pensi alle potenzialità dei moderni dispositivi portatili e all'uso dei social media)*. Ne consegue un grave pregiudizio all'onore e alla dignità della vittima, discendente dalla divulgazione di immagini e/o parole carpite quando la stessa presumeva di partecipare a una comunicazione del tutto privata, in un contesto, cioè, riservato e confidenziale, che tale doveva restare, contro ogni indebita invasione della propria sfera personale ».

La previsione della procedibilità a querela conferma che l'oggetto di tutela dell'articolo 617-*septies* è l'interesse del singolo al mantenimento del proprio onore e della propria reputazione e a evitarne la compromissione a seguito di indebite e non autorizzate divulgazioni all'esterno delle manifestazioni del proprio pensiero, espresse in privato.

Sul piano strutturale, la condotta sanzionata consiste nella diffusione di una captazione fraudolenta, effettuata mediante riprese audio/video o registrazioni, di conversazioni o incontri di tipo privato, alle quali l'agente abbia preso parte o sia stato presente<sup>(112)</sup>.

## 2.2 I rapporti con il c.d. *revenge porn*

La fattispecie in questione pone il tema del raffronto con i reati a sfondo sessuale come quello di « *diffusione illecita di immagini o video sessualmente espliciti* », previsto dall'articolo 612-*ter* che, come ampiamente esposto, si sostanzia nella divulgazione non autorizzata *on line* di *file* multimediali a contenuto sessualmente esplicito, soprattutto a scopo di vendetta nei confronti dell'ex partner.

Peculiarità di questo tipo di immagini e video – oltre alla connotazione del loro contenuto, che deve essere sessualmente esplicito, laddove nel reato di cui all'articolo 617-*septies* assume rilievo la fraudolenta captazione delle immagini/registrazioni di dati sensibili – è che gli stessi sono girati con il consenso della persona ritratta (all'interno di coppie, nell'ambito di momenti intimi consensuali); a essere non consensuale, nel c.d. *revenge porn*, non è la realizzazione del materiale pornografico, ma la sua successiva diffusione.

## 2.3 L'elemento soggettivo

La norma, punendo la fraudolenta ripresa, audio o video, di incontri privati, o la registrazione, anch'essa fraudolenta, di conversazioni, anche telefoniche o telematiche, a cui l'agente abbia preso parte o abbia presenziato, richiede, ai fini della configurazione del reato *de quo*, non la mera diffusione del materiale, bensì che la diffusione avvenga al fine di recare danno all'altrui reputazione o immagine (dolo specifico).

Non sarebbe, ad esempio, sufficiente a integrare il reato la sola diffusione di immagini o registrazioni carpite senza il consenso della vittima, pur supportata dal dolo generico: non è punibile, esemplificando, la condotta di chi abbia « cliccato » sul tasto condividi, richiedendosi il *quid pluris*, sotto il profilo soggettivo, costituito dall'intenzione di danneggiare l'immagine e la reputazione della persona offesa, uno scopo ulteriore verso cui deve tendere la volontà del soggetto agente, una proiezione finalistica, sebbene non se ne richieda, ai fini dell'esistenza della fattispecie, l'effettivo conseguimento<sup>(113)</sup>.

(112) Cass. pen., sez. V, 17 ottobre 2024, n. 2112.

(113) È chiaro che tale finalizzazione della volontà presuppone il dolo – generico – richiesto per la realizzazione dell'evento tipico della fattispecie (diffusione delle immagini o della registrazione), comprensivo quindi, anche del dolo eventuale, ravvisabile nell'accettazione del rischio che la messa in circolazione delle riprese o delle registrazioni fraudolentemente carpite possa determinarne la diffusione.

## 2.4 Le telecamere di videosorveglianza interne alle abitazioni

Diego Marson, Chief Technical Officer di Yarix Var Group<sup>(114)</sup>, ha dichiarato che c'è una scarsa consapevolezza da parte degli utenti dei rischi legati all'installazione delle telecamere IP (*Internet Protocol Camera*)<sup>(115)</sup> ossia dei dispositivi che acquisiscono immagini video in formato digitale e le trasmettono tramite una rete dati.

Spesso questi dispositivi, ad esempio, vengono installati con credenziali di *default* senza che poi venga cambiata successivamente la *password* per l'accesso mettendo così a rischio la *privacy* di chi abita nella casa che vorrebbe rendere più sicura.

Per contenere la rapida diffusione delle immagini e dei video illecitamente captati, occorrono processi rapidi per scambiare le informazioni tra aziende private e Forze dell'ordine nazionali ed estere; è necessaria, inoltre, una cabina di regia per definire le regole e le modalità di questo dialogo e anche una legislazione sovranazionale armonizzata per il contrasto della diffusione dei dati informatici.

### 2.4.1 Gli accorgimenti

Per scongiurare indebite interferenze nella vita privata, viene consigliato di acquistare le telecamere di videosorveglianza da produttori affidabili, da tempo sul mercato, che rilasciano periodicamente degli aggiornamenti di sicurezza.

Occorre, inoltre, accertarsi – come quando si aggiorna il sistema operativo dello *smartphone* o del computer di casa – dell'avvenuto aggiornamento del sistema di sicurezza delle telecamere. Normalmente, l'applicazione per controllare casa, che si installa sul dispositivo mobile, dà la possibilità o di aggiornarla in automatico o, comunque, di verificare gli aggiornamenti disponibili.

Infine, è necessario cambiare le *password* di *default* dei dispositivi non appena vengono installati attivando l'autenticazione a due fattori. Questo offre la possibilità, nel caso in cui, ad esempio, arrivi una mail di *phishing*<sup>(116)</sup> (caso abbastanza frequente), di fare in modo che, chi ha rubato le credenziali, non sia in possesso del secondo fattore di autenticazione e non possa accedere al nostro *account*.

## 3. Il delitto di illecita diffusione di contenuti generati o manipolati con sistemi di intelligenza artificiale

### 3.1 Gli elementi costitutivi

Dal secondo Novecento, la rivoluzione informatica ha assunto una incidenza sulla vita individuale e collettiva tale da configurare una

(114) Audizione del 17 novembre 2025.

(115) Una telecamera IP o *IP cam* è un tipo di videocamera che genera un segnale video in forma digitalizzata e in formato pronto per la trasmissione diretta su rete dati, senza necessità di conversione analogico-digitale, e in grado di essere controllata direttamente tramite la rete dati stessa.

(116) Il *phishing* è una minaccia informatica che mira a ingannare le vittime per ottenere informazioni sensibili, quali credenziali di accesso o dati finanziari. Questo tipo di truffa avviene principalmente attraverso messaggi di posta elettronica ingannevoli che sembrano, a tutti gli effetti, provenire da siti *web* regolari. Quanto alla etimologia, il termine «*phishing*» deriva dalla parola inglese «*fishing*», che significa «pescare». Questo termine è stato adattato per descrivere il modo in cui i truffatori «pescano» informazioni sensibili, come dati finanziari e *password*, ingannando le vittime.

« società digitale » in cui la diffusione del *personal computer*, l'avvento di internet e degli *smartphone*, hanno dilatato l'impiego di strumenti digitali nella quotidianità.

In questo contesto, l'evoluzione tecnologica fa sì che le « macchine » dispongano ormai di margini di auto-apprendimento, auto-organizzazione, auto-decisione. Ne segue che si pone all'etica, al diritto, al dibattito pubblico il tema della « intelligenza artificiale » e di una sua regolazione <sup>(117)</sup>.

La legge 23 settembre 2025, n. 132, « *Disposizioni e deleghe al Governo in materia di intelligenza artificiale* », nel regolamentare l'uso dell'intelligenza artificiale, ha apportato significative novità in materia penale. È stata introdotta una circostanza aggravante comune – che porta a un aumento della pena qualora il reato venga commesso mediante sistemi di intelligenza artificiale – e coniata una nuova fattispecie di reato: l'illecita diffusione di contenuti generati o manipolati con sistemi di intelligenza artificiale.

L'articolo 612-*quater* del codice penale, inserito nell'ambito del titolo XII (Delitti contro la persona), capo III (Delitti contro la libertà individuale), sezione III (Delitti contro la libertà morale), punisce con la reclusione da uno a cinque anni chiunque cagioni un danno ingiusto ad una persona cedendo, pubblicando o diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a trarre in inganno sulla loro genuinità.

Secondo quanto riportato dalla Relazione illustrativa, riferita al disegno di legge originario, il legislatore ha inteso offrire una tutela rafforzata della persona, incentrando l'offensività della condotta sul pregiudizio all'autodeterminazione e al pieno svolgimento della personalità, circostanza confermata anche dalla collocazione sistematica della disposizione fra i delitti contro la persona e, segnatamente contro la libertà morale.

Il delitto, inoltre, è punibile a querela ma si procede d'ufficio se il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio ovvero se il fatto è commesso nei confronti di persona incapace, per età o infermità, o nei confronti di una pubblica autorità a causa delle funzioni esercitate.

Per il Dirigente superiore della Polizia di Stato, *Ivano Gabrielli*, Direttore del Servizio Polizia postale e per la sicurezza cibernetica <sup>(118)</sup>,

(117) Come evidenziato da *Sandra Cioffi*, Presidente del Consiglio Nazionale degli Utenti, a pagina 2 della memoria fatta pervenire il 29 gennaio 2026, « *se i sistemi di IA vengono addestrati prevalentemente su testi, narrazioni e cronache che rappresentano la violenza di genere come evento ricorrente, relazioni fondate sul possesso o sulla gelosia, esiste il rischio che tali modelli riflettano e riproducano implicitamente queste rappresentazioni, contribuendo alla loro diffusione nello spazio digitale. Diventa pertanto essenziale interrogarsi sul rapporto tra tecnologia, contenuti e responsabilità culturale, affinché l'innovazione digitale non rafforzi stereotipi e narrazioni distorte, ma sia orientata alla tutela dei diritti fondamentali e alla prevenzione della violenza. Per queste ragioni appare indispensabile: affiancare allo sviluppo tecnologico una riflessione etica e culturale strutturata; introdurre criteri di selezione e bilanciamento dei dati di addestramento dei sistemi di intelligenza artificiale; promuovere rappresentazioni delle relazioni di genere fondate sul rispetto, sull'autonomia e sulla reciprocità; rafforzare la comunicazione e l'educazione ai media e al digitale come strumenti centrali di prevenzione della violenza di genere* ».

(118) Audizione del 17 novembre 2025.

si tratta di una norma in linea con la storia giuridica del nostro ordinamento.

L'Italia è uno dei pochi Paesi che, già da tempo, ha introdotto il reato di pedopornografia virtuale. Si è compreso che il disvalore di un'immagine artificialmente prodotta non è di minor conto e di minor peso rispetto a quello di un'immagine reale dal vivo. Questo è un atto di civiltà importantissimo che ci pone all'avanguardia nella tutela dei minori. Questa tipologia di reati ci permette di perseguire gli autori dei c.d. « abusi sintetici », compresa la violenza sessuale ai danni di minori.

La legge prevede pene più severe se l'intelligenza artificiale viene utilizzata come mezzo insidioso, ponendo la vittima in una condizione di minorata difesa, o come strumento per manipolare i diritti politici o per realizzare frodi finanziarie, come l'aggiotaggio e la manipolazione del mercato. L'introduzione del delitto di illecita diffusione di contenuti generati o manipolati con sistemi di intelligenza artificiale segna un confine netto tra l'uso lecito e illecito della tecnologia. L'IA (l'intelligenza artificiale) non è di per sé pericolosa: lo diventa quando manca la responsabilità di chi la usa.

*Lucia Bainotti, Assistant Professor in Digital and Visual Media Analysis* presso il Dipartimento di *Media Studies* dell'Università di Amsterdam <sup>(119)</sup>, ha raccontato che, sul sito *Phica.eu*, erano presenti sezioni dedicate a dare suggerimenti su come creare contenuti con l'intelligenza artificiale e come condividerli; è estremamente semplice caricare foto e produrre foto di nudo che, pur essendo generate sinteticamente, producono effetti concreti per le persone rappresentate che vedono la loro vita quotidiana, individuale, condizionata da queste immagini e dalla loro condivisione. Si è registrato un aumento della creazione di *bot* <sup>(120)</sup> su *Telegram* <sup>(121)</sup>, non solo per sponsorizzare i servizi di creazione di immagini sintetiche non consensuali, ma anche per generarli.

*Silvia Semenzin* <sup>(122)</sup> ha ricordato che le nuove forme di diffusione non consensuale di materiale intimo, come per esempio quelle facilitate dalla tecnologia dell'intelligenza artificiale generativa (il cosiddetto *deepfake* sessuale), riguardano, nel 99% dei casi, donne. Si tratta di tecnologie che non « funzionano » sui corpi maschili, « funzionano » solo sui corpi femminili. Questo fa capire quanto effettivamente la matrice di genere esista anche perché, poi, di tutti i *deepfake* che si trovano *on line*, il 96% sono di natura pornografica. Si tratta di un problema in rapida ascesa, considerato che, dal 2023, i *deepfake* sono aumentati del 550%.

(119) Audizione del 17 novembre 2025.

(120) Un « *bot* », abbreviazione di « *robot* », è un programma informatico progettato per eseguire compiti specifici in modo autonomo, spesso imitando il comportamento umano in vari contesti *on line*. Questi programmi *software* possono navigare su internet, inviare messaggi, raccogliere dati e svolgere molte altre funzioni senza l'intervento umano diretto. I *bot* di *Telegram*, in particolare, possono essere considerati come utenti artificiali che operano all'interno dell'applicazione essendo programmati per eseguire azioni specifiche e interagire con gli utenti in modo « amichevole ».

(121) *Telegram* è un'applicazione di messaggistica che offre *chat* crittografate, canali, gruppi, *bot*.

(122) Audizione del 16 ottobre 2025.

### 3.2 « Non con la mia faccia. #IoDenuncio »

L'associazione Giornaliste italiane<sup>(123)</sup> ha promosso una azione collettiva per denunciare l'abuso delle immagini delle donne modificate e manipolate con l'intelligenza artificiale.

Il messaggio « Non con la mia faccia » significa rifiutare che il volto o l'identità di una persona vengano usati per scopi contrari alla dignità e alla verità dopo i recenti casi. Una dichiarazione collettiva contro una forma di violenza che non lascia lividi, ma lacera l'identità: la pornografia *deepfake*. Là dove il potere tecnologico incontra la cultura dell'abuso, nascono immagini e video costruiti con intelligenza artificiale capaci di replicare i volti delle donne e inserirli, senza alcun consenso, in contenuti pornografici tanto sofisticati quanto falsi.

Volti di donne, noti o no, vengono sottratti da fotografie pubbliche, da profili *social*, da apparizioni televisive e manipolati digitalmente fino a diventare corpi mai esistiti in scene che simulano violenza, sessualità, sottomissione. Queste immagini, indistinguibili dalla realtà, vengono diffuse in silenzio, tra piattaforme *hard* e circuiti criptati. Lo spettatore spesso ignora che si tratta di un falso; la vittima, invece, si ritrova improvvisamente privata della propria immagine, del proprio corpo, della propria credibilità.

Un abuso senza contatto, ma non senza conseguenze.

Piattaforme e siti dedicati macinano visualizzazioni e normalizzano l'abuso: un'inchiesta ha contato quasi 4.000 celebrità coinvolte e 100 milioni di *views* in tre mesi. Se lo fanno ai volti famosi, possono farlo a chiunque. Questo non è un fenomeno marginale, ma un fronte di guerra invisibile. Un conflitto contro il corpo femminile, condotto nel silenzio algoritmico della rete.

Ciò che si combatte non è soltanto un abuso tecnologico, ma una visione radicata e persistente: quella che considera il corpo della donna accessibile, rappresentabile, riproducibile, indipendentemente dalla sua volontà. Una logica che sottrae l'immagine alla persona per farne oggetto di consumo. Il *deepfake* pornografico non è una devianza della tecnologia, ma la sua complicità con un'antica forma di violenza simbolica. Si ruba un volto, ma si ferisce l'intera identità. Si crea finzione, ma si genera un danno concreto. Nulla, in questa operazione, è virtuale. Non si tratta di progresso, ma di dominio che si traveste da innovazione. E non può essere tollerato<sup>(124)</sup>.

(123) *Giornaliste italiane* nasce con l'intento di promuovere azioni mirate alla valorizzazione delle donne, alla loro crescita in tutti i campi professionali, al raggiungimento di una piena parità di genere sia nell'occupazione sia nella crescita professionale. L'associazione ha l'ambizione di diventare un manifesto culturale per tutte le giornaliste libere: libere dalle appartenenze, libere dai pregiudizi, libere dalle catene del conformismo linguistico-culturale del politicamente corretto e dalle relative derive censorie e persecutorie.

(124) Fabrizia Arcuri, *Flash mob contro l'uso non consensuale di volti femminili in contenuti porno con l'IA. Non con la mia faccia: Giornaliste Italiane in piazza*, 5 novembre 2025, in <https://www.giornalistitalia.it/non-con-la-mia-faccia-giornaliste-italiane-in-piazza/> da cui è tratta la foto. A Roma, in occasione del *flashmob* organizzato a Piazza Capranica, non si è semplicemente manifestato: si è preso atto, con fermezza e lucidità, che l'abuso dell'immagine femminile attraverso contenuti pornografici generati con IA è una violenza che pretende risposta.



*Flash mob contro l'uso non consensuale di volti femminili in contenuti porno con l'IA. Non con la mia faccia: Giornaliste Italiane in piazza, 5 novembre 2025, Roma, Piazza Capranica.*

#### **4. Il trattamento illecito di dati personali**

##### **4.1 I dati personali**

I dati personali sono le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica.

Particolarmente importanti sono: i dati che permettono l'identificazione diretta – come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. –; i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa); i dati rientranti in particolari categorie: si tratta dei dati c.d. «sensibili», cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale.

L'articolo 9 del Regolamento 2016/679/UE del 27 aprile 2016 (c.d. *GDPR – General Data Protection Regulation*) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale; i dati relativi a condanne penali e reati.

Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

##### **4.2 Gli elementi costitutivi del reato**

L'articolo 167 del decreto legislativo n. 196 del 2003 (Codice in materia di protezione dei dati personali) prevede, al primo comma, che,

salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 dello stesso codice o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.

Il secondo comma dispone che, salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del GDPR in violazione delle disposizioni di cui agli articoli 2-*sexies* e 2-*octies* o delle misure di garanzia di cui all'articolo 2-*septies* del codice arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni <sup>(125)</sup>.

#### 4.2.1 Il bene giuridico tutelato

Nel delitto di trattamento illecito di dati personali, il bene giuridico si identifica nella riservatezza, che coincide con il diritto dell'individuo a preservare la propria sfera personale dalle attenzioni di quanti non abbiano titolo per ingerirsi in essa ed attiene, quindi, all'aspetto interiore dell'individuo, che ha diritto a proteggersi dalle indiscrezioni altrui.

#### 4.2.2 Il nocumento

L'attuale formulazione della norma è frutto delle modifiche apportate dal decreto legislativo 10 agosto 2018, n. 101, recante « *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)* ».

A seguito della riforma, il primo comma dell'art. 167 cit. non fa più riferimento al trattamento e introduce l'elemento del danno all'interessato – che connota anche il dolo specifico – costituito dal pregiudizio, anche di natura non patrimoniale, subito dalla persona cui si riferiscono i dati quale conseguenza dell'illecito trattamento <sup>(126)</sup>.

La nozione di nocumento, in definitiva, coerentemente con l'etimologia del termine (derivante dal verbo nuocere, ovvero arrecare un danno fisico o morale), evoca l'esistenza di una concreta lesione della sfera personale o patrimoniale che deve ritenersi direttamente riconducibile a un'operazione di illecito trattamento dei dati protetti.

(125) Il Pubblico ministero, quando ha notizia del reato ne informa senza ritardo il Garante. Quest'ultimo trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni del codice della *privacy*. Quando per lo stesso fatto è stata applicata a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

(126) Cass. pen., sez. III, 7 febbraio 2017, n. 29549.

#### **4.2.3 La pubblicazione di una foto altrui sui social**

Il consenso all'uso dell'immagine come foto profilo *WhatsApp* non equivale affatto a una diffusione indiscriminata cosicché, la successiva pubblicazione della stessa su un gruppo *Facebook*, accessibile a un pubblico molto più ampio e in un contesto denigratorio, integra una condotta di trattamento illecito di dati personali<sup>(127)</sup>.

L'ulteriore diffusione della foto senza consenso, in particolare in contesti ostili o minacciosi, comporta un autonomo e grave *vulnus* alla riservatezza della persona ritratta.

#### **4.3 La diffusione del numero di telefono di una persona mediante il suo inserimento in una chat a contenuto erotico**

Anche colui che diffonde il numero di telefono cellulare di altra persona, mediante il suo inserimento in una *chat* a contenuto erotico con invito a contattare l'utenza per prestazioni sessuali, al fine di arrecare danno all'interessato, risponde del reato di illecito trattamento di dati personali<sup>(128)</sup>.

#### **4.4 La diffusione su siti porno di fotomontaggi utilizzando foto prelevate da Facebook**

È parimenti configurabile il trattamento illecito di dati personali nel caso in cui taluno, anche solo per un breve lasso di tempo, posta su siti porno fotomontaggi realizzati a partire da foto prelevate da *Facebook*<sup>(129)</sup>.

La divulgazione delle fotografie delle ragazze su siti *hard* comporta la lesione della loro onorabilità: l'esposizione delle foto manipolate, ai commenti degli utenti dei siti pornografici, arreca un evidente e non lieve nocumento alla reputazione delle persone ritratte.

### **5. La sostituzione di persona**

#### **5.1 Gli elementi costitutivi**

L'articolo 494 codice penale punisce con la reclusione fino a un anno chiunque, al fine di procurare a sé o ad altri<sup>(130)</sup> un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge

(127) Cass. pen., sez. V, 14 luglio 2025, n. 29683.

(128) Cass. pen., sez. III, 24 ottobre 2019, n. 46376. Nello stesso senso Cass. pen., sez. III, 24 ottobre 2019, n. 46376, secondo cui integra il reato di trattamento abusivo dei dati di traffico, tra i quali rientra il numero dell'utenza cellulare, la condotta consistita nel registrare quest'ultimo in una *chat* a contenuto erotico all'insaputa del suo titolare.

(129) Cass. pen., sez. III, 19 giugno 2019, n. 43534. Nel caso di specie, l'imputato aveva diffuso su due siti pornografici, senza alcun preventivo consenso, le immagini di diverse ragazze di sua conoscenza, dopo averle in molti casi manipolate, incitando gli utenti dei siti a « commentare » le immagini caricate. Ben presto le vittime dell'indebita diffusione delle immagini, legate peraltro da legami di reciproca conoscenza, sono venute a conoscenza dell'accaduto e non hanno esitato a sporgere querela, venendo poi rimossi in tempi rapidi dai due siti i contenuti visivi.

(130) Cass. pen., sez. V, 5 febbraio 2021, n. 12062.

attribuisce effetti giuridici, se il fatto non costituisce un altro delitto contro la fede pubblica.

La norma tutela la fede pubblica in quanto può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali; siccome si tratta di inganni che possono superare la ristretta cerchia d'un determinato destinatario, il legislatore ha ravvisato in essi una costante insidia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome<sup>(131)</sup>.

La giurisprudenza di legittimità, seguendo l'evoluzione di abitudini sociali e tempi storici, ha già ripetutamente affermato che il reato di sostituzione di persona è configurabile nella condotta di colui che crei e utilizzi *account* o profili di *social network* ovvero *sim card* a nome di altro soggetto, inconsapevole, servendosi dei suoi dati personali, con il fine di far ricadere su quest'ultimo il suo agire<sup>(132)</sup>.

## 5.2 Il concorso con il delitto di trattamento illecito di dati personali

Il delitto di sostituzione di persona concorre con quello di trattamento illecito di dati personali, stante la diversa oggettività giuridica delle fattispecie: il primo tutela la fede pubblica, il secondo la riservatezza, che ha riguardo all'aspetto interiore dell'individuo e al suo diritto a preservare la propria sfera personale da indiscrezioni e attenzioni indebite, pur potendo ricorrere tra le due fattispecie omogeneità della condotta realizzativa<sup>(133)</sup>.

Il delitto di sostituzione di persona è integrato dalla creazione e utilizzazione di un « profilo » su « *social network* » servendosi abusivamente dell'immagine di un'altra persona inconsapevole, in quanto idonea alla rappresentazione di un'identità digitale non corrispondente al soggetto che ne fa uso<sup>(134)</sup>. La descrizione di un profilo poco lusinghiero sul « *social network* » evidenzia sia il fine di vantaggio, consistente nell'agevolazione delle comunicazioni e degli scambi di contenuti in rete, sia il fine di danno per il terzo, di cui è abusivamente utilizzata l'immagine<sup>(135)</sup> e comporta che gli utilizzatori del servizio vengano tratti in inganno sulla disponibilità della persona associata all'immagine a ricevere comunicazioni a sfondo sessuale o sentimentale<sup>(136)</sup>.

L'ostensione di dati personali del titolare ai frequentatori di un *social network*, attraverso l'inserimento degli stessi, previa creazione di

(131) Cass. pen., sez. V, 8 novembre 2007, n. 46674.

(132) Cfr. Cass. pen., sez. V, 13 luglio 2020, n. 25215; Cass. pen., sez. V, 23 aprile 2014, n. 25774; Cass. pen., sez. V, 6 luglio 2020, n. 22049; Cass. pen., sez. III, 15 dicembre 2011, n. 12479. V. anche Cass. pen., sez. V, 20 settembre 2022, n. 41801 secondo cui integra l'ipotesi di sostituzione di persona la condotta di chi crea un profilo falso su un *social network* utilizzando i riferimenti della persona offesa così inducendo in errore coloro che comunicano con lui attraverso la chat e determinandoli a recare disturbo o molestia alla vittima e Cass. pen., sez. V, 14 ottobre 2021, n. 323 che ha ravvisato il reato nella condotta di colui che crei ed utilizzi « profili *social* » e « *account internet* » servendosi dei dati anagrafici di altra persona, esplicitamente contraria, al fine di far ricadere su quest'ultima l'attribuzione delle connessioni eseguite in rete.

(133) Come chiarito da Cass. pen., sez. V, 5 febbraio 2021, n. 12062 affrontando il caso dell'utilizzo dell'immagine di una persona ignara e non consenziente per la creazione di un falso profilo su un « *social network* ».

(134) Cass. pen., sez. V, 6 luglio 2020, n. 22049.

(135) Cass. pen., sez. V, 23 aprile 2014, n. 25774.

(136) Cass. pen., sez. V, 28 novembre 2012, n. 18826.

un falso profilo, sul relativo sito<sup>(137)</sup>, integra anche il reato di illecito trattamento dei dati personali<sup>(138)</sup>.

## 6. La diffamazione

### 6.1 Gli elementi costitutivi

L'articolo 595 del codice penale punisce con la reclusione fino a un anno o con la multa fino a 1.032 euro chiunque, comunicando con più persone, offende l'altrui reputazione<sup>(139)</sup>.

Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a 516 euro.

Il reato sussiste anche quando la propalazione offensiva dell'altrui onore e decoro intervenga non contemporaneamente nei confronti di più persone, ma in tempi diversi<sup>(140)</sup>.

Il bene giuridico si identifica nella reputazione che coincide con la considerazione, in relazione al sentire del momento storico, di cui la persona gode nell'ambiente sociale ed attiene, quindi, all'aspetto esteriore dell'individuo, che ha diritto a godere, appunto, di un certo riconoscimento sociale.

### 6.2 La presenza virtuale

La differenza fra l'ingiuria, ora non prevista più come reato, e il delitto di diffamazione risiede nella presenza ovvero assenza del destinatario delle espressioni offensive: mentre nell'ingiuria la comunicazione, con qualsiasi mezzo realizzata, è diretta all'offeso, nella diffamazione l'offeso resta estraneo alla comunicazione offensiva intercorsa con più persone e non è posto in condizione di interloquire con l'offensore<sup>(141)</sup>.

Diviene dunque dirimente, ai fini della sussistenza del reato, delineare il concetto di « presenza ». Se tradizionalmente esso implica necessariamente la presenza fisica, in unità di tempo e di luogo, di offeso e terze persone, i moderni sistemi tecnologici ne rendono necessaria una specificazione, consentendo questi di realizzare situazioni in cui si può ravvisare una presenza virtuale del destinatario delle affermazioni offensive, sostanzialmente equiparabili alla presenza fisica (quali *conference*, audioconferenza o videoconferenza)<sup>(142)</sup>.

Per tale motivo occorre procedere ad una valutazione caso per caso: se l'offesa viene profferita nel corso di una riunione a distanza (o « da remoto »), tra più persone contestualmente collegate, alla quale partecipa anche l'offeso, ricorrerà l'ipotesi della ingiuria commessa alla presenza di più persone<sup>(143)</sup>; di contro, laddove vengano in rilievo

(137) Cass. pen., sez. III, 28 maggio 2019, n. 42565.

(138) Cass. pen., sez. III, 19 giugno 2018, n. 52135.

(139) La pena è raddoppiata se l'offesa consiste nell'attribuzione di un fatto determinato.

(140) Cass. pen., sez. V, 4 novembre 2010, n. 7408.

(141) Cass. pen., sez. V, 17 gennaio 2019, n. 10313.

(142) Cass. pen., sez. V, 6 luglio 2018, n. 34484; Cass. pen., sez. V, 4 marzo 2021, n. 13252.

(143) Cass. pen., sez. V, 25 febbraio 2020, n. 10905.

comunicazioni (scritte o vocali), indirizzate all'offeso e ad altre persone non contestualmente presenti (nell'accezione estesa alla presenza « virtuale » o « da remoto »), ricorreranno i presupposti della diffamazione, come la giurisprudenza di legittimità ha più volte affermato nel caso, per esempio, all'invio di e-mail<sup>(144)</sup>, ovvero dell'invio di messaggi contenenti espressioni offensive nei confronti della persona offesa su una « chat » condivisa anche da altri soggetti, quando la prima non li abbia percepiti nell'immediatezza, in quanto non collegata al momento del loro recapito<sup>(145)</sup>.

Si configura il delitto di diffamazione, ove manchi la possibilità di interlocuzione diretta tra autore e destinatario dell'offesa, che resti privato della possibilità di replica, vale a dire quando tra l'offensore e l'offeso non sia possibile instaurare un rapporto diretto, reale o virtuale, che garantisca a quest'ultimo un contraddittorio immediato, con possibilità di replica<sup>(146)</sup>.

Le situazioni equiparate alla presenza fisica devono essere caratterizzate da un rapporto diretto tra offensore e offeso, il quale non sussiste nell'ipotesi di comunicazione attraverso il mezzo televisivo o un *social media*<sup>(147)</sup>.

### **6.3 La diffusione di un messaggio diffamatorio attraverso l'uso di un *social network* (come *Instagram* o *Facebook*)**

La diffusione di un messaggio diffamatorio attraverso l'uso di un « *social network* » (come « *Instagram* » o « *Facebook* ») integra un'ipotesi di diffamazione aggravata poiché la condotta in tal modo realizzata è potenzialmente capace di raggiungere un numero indeterminato, o comunque quantitativamente apprezzabile, di persone<sup>(148)</sup>.

### **6.4 Il rapporto con il reato di *stalking*...**

Il delitto di atti persecutori concorre con quello di diffamazione anche quando nelle modalità della condotta diffamatoria si esprimono le molestie reiterate costitutive del reato di atti persecutori: ciò in quanto, pur volendo considerare i comportamenti denigratori come espressione delle condotte moleste necessarie a integrare il delitto di atti persecutori, l'evento tipico di quest'ultimo reato, ossia l'effetto destabilizzante della serenità e dell'equilibrio psicologico della vittima, differisce da quello del delitto di diffamazione, che si identifica nella

(144) Cass. pen., sez. V, 4 marzo 2021, n. 13252; Cass. pen., sez. V, 6 aprile 2011, n. 29221.

(145) Cass. pen., sez. V, 10 giugno 2022, n. 28675.

(146) Cfr., *ex plurimis*, Cass. pen., sez. VI, 23 marzo 2023, n. 17563.

(147) Integra il delitto di diffamazione, aggravato da mezzo di pubblicità diverso dalla stampa, la dichiarazione offensiva resa nel corso di un video pubblicato sui *social media* al quale il destinatario non sia presente fisicamente, ma abbia assistito « in diretta da remoto », atteso che la possibilità di inserire « commenti » non assicura un rapporto diretto con l'offensore né un contraddittorio immediato ed in forme adeguate, rispettose di una sostanziale « parità delle armi » (Cass. pen., sez. V, 5 giugno 2025, n. 29458).

(148) Cass. pen., sez. V, 25 gennaio 2021, n. 13979; Cass. pen., sez. I, 28 aprile 2015, n. 24431; Cass. pen., sez. V, 14 novembre 2016, n. 4873; Cass. pen., sez. V, 7 maggio 2024, n. 34057.

diffusione di dati capaci di gettare discredito sull'immagine globale della persona cui quelli si riferiscano <sup>(149)</sup>.

#### **6.4.1 ... e di trattamento illecito di dati personali**

È configurabile il concorso tra il delitto di trattamento illecito di dati personali e quello di diffamazione perché, mentre quest'ultimo protegge la reputazione, attinente all'aspetto esteriore della tutela dell'individuo e al suo diritto di godere di un certo riconoscimento sociale, il primo è posto a tutela della riservatezza che ha riguardo all'aspetto interiore dell'individuo e al suo diritto a preservare la propria sfera personale da ingerenze indebite <sup>(150)</sup>.

### **7. La truffa**

#### **7.1 Gli elementi costitutivi**

L'articolo 640 del codice penale punisce con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno.

Il giudizio sull'idoneità della condotta a trarre in inganno la persona offesa dev'essere effettuato *ex post* e in concreto, sicché la non particolare raffinatezza degli artifici utilizzati, ovvero lo stato di vulnerabilità della vittima, non escludono l'offensività della condotta <sup>(151)</sup>.

#### **7.2 La truffa telematica**

Ricorre l'ipotesi di truffa telematica quando il fatto è commesso a distanza attraverso strumenti informatici o telematici, idonei ad ostacolare la propria o l'altrui individuazione e ciò si concretizza in tutte le ipotesi in cui lo strumento della rete viene utilizzato per impedire alla vittima l'identificazione del responsabile <sup>(152)</sup>. La pena, in questo caso, è più elevata (reclusione da uno a cinque anni e multa da 309 euro a 1.549 euro).

La legge 28 giugno 2024, n. 90, introducendo la nuova circostanza aggravante del delitto di truffa telematica, ha in sostanza recepito l'elaborazione giurisprudenziale che riteneva applicabile la circostanza aggravante « comune » dell'articolo 61, n. 5 del codice penale all'ipotesi delle truffe commesse « a distanza » sfruttando lo strumento della rete proprio al fine di rendere più difficoltosa o addirittura impossibile, da parte della vittima, la identificazione del suo interlocutore.

Si è infatti ripetutamente affermato che, in caso di truffe commesse « a distanza » con il mezzo telematico, è proprio la distanza tra il luogo ove si trova il *deceptus* e quello in cui opera l'agente, che è tale da determinare una posizione di vantaggio per l'agente, consentendogli di

(149) Cass. pen., sez. V, 25 febbraio 2025, n. 12282.

(150) Cass. pen., sez. V, 2 maggio 2019, n. 30455.

(151) Cass. pen., sez. II, 23 settembre 2025, n. 3290.

(152) Cass. pen., sez. II, 2 aprile 2025, n. 14217.

schermare la sua identità e di sottrarsi agevolmente alle conseguenze della propria condotta<sup>(153)</sup>.

Il legislatore, allora, ha « enucleato », dalla fattispecie descritta al n. 5 dell'articolo 61, una ipotesi specifica di « minorata difesa » individuata, per l'appunto, nella situazione del truffatore che, nel contattare e interloquire con la vittima, strumentalizza il mezzo telematico per garantirsi una posizione di vantaggio: in altri termini, ha « sottratto » dall'articolo 61 n. 5 l'ipotesi della truffa telematica cui ha riservato una considerazione autonoma<sup>(154)</sup>.

### 7.3 Il rapporto con il reato di illecito trattamento dei dati personali

Il reato di truffa e quello di illecito trattamento dei dati personali possono concorrere in quanto sono integrati da condotte diverse (perché l'illecito trattamento dei dati personali prescinde dall'uso di artifici e raggiri, dall'induzione in errore e dal nesso causale tra il profitto e il danno e, inoltre, il fine di profitto è alternativo a quello di provocare un nocumento) e sono caratterizzati da un diverso elemento soggettivo (essendo richiesto il dolo specifico solo per la configurabilità del delitto previsto dall'articolo 167 del decreto legislativo n. 196 del 2003)<sup>(155)</sup>.

## 8. La violenza sessuale virtuale

### 8.1 Gli elementi costitutivi

Si è progressivamente affermato un filone giurisprudenziale<sup>(156)</sup> che, partendo dalla considerazione secondo cui « la sfera della sessualità non resta confinata sul piano strettamente fisico, ma involge anche la sfera psichica e quella emotiva, suscettibile di modularsi diversamente in relazione ai valori del comune sentire che si consolidano nello specifico contesto storico, culturale e sociale di riferimento », ha progressivamente « sublimato » la nozione di « atti sessuali », includendovi casi in cui il corpo della vittima non viene fisicamente aggredito dall'agente di reato, ma nei quali il contesto dell'azione consenta di affermare che la condotta dell'agente ha comunque inciso nella sfera di autodeterminazione sessuale della vittima. Si è quindi ritenuto che il reato di violenza sessuale possa essere commesso anche « a distanza », ovvero sia a mezzo telefono o di altre apparecchiature di comunicazione elettronica<sup>(157)</sup>, in quanto la norma incriminatrice non richiede, all'in-

(153) Cfr., in tal senso, tra le tante, Cass. pen., sez. II, 2 luglio 2024, n. 31825; Cass. pen., sez. II, 6 giugno 2024, n. 25968; Cass. pen., sez. II, 10 aprile 2024, n. 20165; Cass. pen., sez. II, 18 gennaio 2024, n. 11150; Cass. pen., sez. II, 6 dicembre 2023, n. 50005; Cass. pen., sez. II, n. 27132 del 2023; Cass. pen., sez. II, 28 ottobre 2022, n. 2585; Cass. pen., sez. II, 8 aprile 2021, n. 28070; Cass. pen., sez. II, 4 dicembre 2019, n. 51551; Cass. pen., sez. VI, 22 marzo 2017, n. 17937; Cass. pen., sez. II, 29 settembre 2016, n. 43706.

(154) Cass. pen., sez. II, 9 maggio 2025, n. 22257.

(155) Cass. pen., sez. III, 19 giugno 2018, n. 52135.

(156) Cass. pen., sez. III, 18 settembre 2019, n. 43423.

(157) Cass. pen., sez. III, 18 luglio 2012, n. 37076; Cass. pen., sez. III, 3 dicembre 2008, n. 12987. Se è pacifico che non sia necessaria ai fini del compimento di un atto sessuale la presenza fisica dell'agente, elemento non solo richiesto dalla *littera legis*, ma configurante una connotazione quanto meno anacronistica in una realtà quale quella attuale sempre più improntata a relazioni di natura virtuale legate all'interconnessione

terno dell'elemento oggettivo del reato, che tra soggetto attivo e passivo vi sia contestualità spaziale, ben potendo la minaccia o la violenza essere posta anche in luogo diverso da quello in cui il soggetto passivo la subisce, essenziale invece essendo che la costrizione venga, da quest'ultima, effettivamente percepita <sup>(158)</sup>.

E invero, se è pacifico che non sia necessaria ai fini del compimento di un atto sessuale la presenza fisica dell'agente, elemento non solo non richiesto dalla *littera legis*, ma configurante una connotazione quanto meno anacronistica in una realtà quale quella attuale sempre più improntata a relazioni di natura virtuale legate all'interconnessione telematica universalmente apprestata dalla rete che consente la presenza degli interlocutori indipendentemente dalle distanze fisiche o geografiche, diventa un fuor d'opera esigerne la compresenza anche solo telematica al compimento dell'atto, rivolto nei confronti della sua stessa persona da parte della vittima allorquando sia accertato che il suo verificarsi, lungi dal rispondere a una volizione spontanea del suo autore, sia l'effetto della costrizione ovvero dell'induzione posta in essere nei suoi confronti dal suo interlocutore. È, infatti, il coinvolgimento della vittima l'elemento caratterizzante il reato di violenza sessuale in cui la persona offesa finisce per assecondare la volontà dell'agente sottostando ai suoi voleri nell'impossibilità o di sovrastarne la violenza fisica o psichica ovvero di resistere alla *vis* induttiva esprimendo un consenso *in nuce* viziato dall'attività di persuasione svolta nei suoi confronti, essendo in entrambi i casi lesa la sua libertà di autodeterminazione nel compimento dell'atto sessuale <sup>(159)</sup>.

Al riguardo va premesso che il reato di violenza sessuale può configurarsi indipendentemente da un contatto fisico tra l'agente e la vittima allorquando venga lesa la capacità di autodeterminazione di quest'ultima per essere stata costretta, mediante violenza o minaccia, ovvero indotta alla profanazione della sua sfera sessuale. Ricorrono in tal caso inequivocabilmente tutti gli elementi costitutivi della fattispecie delittuosa, ivi compresa la sussistenza dell'atto sessuale per la configurabilità del quale non è affatto richiesto il collegamento fisico tra i due protagonisti, essendo sufficiente il coinvolgimento corporeo del soggetto passivo il quale deve essere, secondo l'espressa formulazione della norma, costretto o indotto a compierli o a subirli per soddisfare, indipendentemente dalla zona corporea attinta e dalla realizzazione della finalità di appagamento dei propri istinti libidinosi da parte dell'agente, le richieste di quest'ultimo.

In altra sentenza, la Suprema Corte ha ritenuto che « la fattispecie criminosa di violenza sessuale è integrata, pur in assenza di un contatto fisico diretto con la vittima, quando gli "atti sessuali" coinvolgano oggettivamente la corporeità sessuale della persona offesa e siano

---

telematica universalmente apprestata dalla rete che consente la presenza degli interlocutori indipendentemente dalle distanze fisiche o geografiche, diventa un fuor d'opera esigerne la compresenza anche solo telematica al compimento dell'atto, rivolto nei confronti della sua stessa persona da parte della vittima allorquando sia accertato che il suo verificarsi, lungi dal rispondere ad una volizione spontanea del suo autore, sia l'effetto della costrizione ovvero dell'induzione posta in essere nei suoi confronti dal suo interlocutore (Cass. pen., sez. III, 21 novembre 2025, n. 41646).

(158) Cass. pen., sez. III, 21 marzo 2006, n. 15158, in un caso di prestazioni sessuali eseguite in videoconferenza via *web-chat*.

(159) Cass. pen., sez. III, 18 settembre 2024, n. 5688.

finalizzati ed idonei a compromettere il bene primario della libertà individuale, nella prospettiva del reo di soddisfare od eccitare il proprio istinto sessuale »<sup>(160)</sup>.

Per la più recente giurisprudenza, tuttavia, anche alla luce della normativa sovranazionale, il concetto di costringere taluno a « subire » atti sessuali non può essere dilatato fino a ricomprendere casi caratterizzati certamente dalla lesione al bene giuridico tutelato, ma anche dalla completa assenza di corporeità, ostando il principio di tassatività a estendere la nozione del « *pati* » fino a ricomprendervi il mero assistere all'atto sessuale altrui<sup>(161)</sup>.

## 9. Il *cyberstalking*

### 9.1 Gli elementi costitutivi

Lo *stalking on line* o *cyberstalking* consiste nell'utilizzo delle tecnologie dell'informazione e della comunicazione per perseguire, intimidire o molestare una persona attraverso comportamenti reiterati e indesiderati.

Il *cyberstalking* è integrato da quei comportamenti che, attraverso l'uso delle nuove tecnologie e della comunicazione mediata dal computer, vengono messi in atto da offensori, definiti *cyberstalker*, con lo scopo di perseguire le vittime, in modo sistematico e abituale.

Le condotte persecutorie digitali possono manifestarsi attraverso molteplici canali: email indesiderate, messaggi ossessivi sui *social network*, commenti molesti su piattaforme digitali, monitoraggio delle attività *on line* e creazione di profili falsi per aggirare i blocchi eventualmente imposti dalla vittima esasperata.

Ai fini della configurabilità del delitto di *stalking*, non rileva la presenza della persona offesa alle minacce o molestie<sup>(162)</sup> né la direzione immediata della condotta persecutoria nei suoi riguardi, ove vi sia consapevolezza, da parte dell'agente, del fatto che delle minacce e/o delle molestie la vittima venga informata e, d'altra parte, vi sia consapevolezza della idoneità del proprio comportamento abituale a produrre uno degli eventi alternativamente previsti dalla norma incriminatrice<sup>(163)</sup>.

La pena è aumentata se il fatto è commesso attraverso strumenti informatici o telematici.

Integrano il delitto di atti persecutori, le condotte di reiterate molestie attuate sostituendosi alla vittima tramite profili *social* e *account* internet falsamente a lei riconducibili, mediante i quali l'agente faccia credere a terzi sconosciuti che costei sia disponibile ad approcci sessuali, tanto da far sì che costoro la avvicinino ripetutamente nei luoghi da lei frequentati<sup>(164)</sup>.

La consapevolezza dell'idoneità lesiva del proprio comportamento è condizione necessaria e sufficiente a integrare il reato, poiché il

(160) Cass. pen., sez. III, 18 settembre 2014, n. 39904, che richiama Cass. pen., sez. III, 24 marzo 2011, n. 11958.

(161) Cass. pen., sez. III, 21 ottobre 2025, n. 37942.

(162) Cass. pen., sez. III, 6 ottobre 2015, n. 1629.

(163) Cass. pen., sez. V, 16 febbraio 2021, n. 8919.

(164) Cass. pen., sez. V, 14 ottobre 2021, n. 323.

delitto di atti persecutori è fattispecie a dolo generico, il cui contenuto richiede la volontà di porre in essere più condotte di minaccia e molestia, nella consapevolezza della loro idoneità a produrre uno degli eventi alternativamente previsti dalla norma incriminatrice e dell'abitudine del proprio agire, ma non postula la preordinazione di tali condotte — elemento non previsto sul fronte della tipicità normativa — potendo queste ultime, invece, essere in tutto o in parte anche meramente casuali e realizzate qualora se ne presenti l'occasione<sup>(165)</sup>.

## 10. La istigazione al suicidio

### 10.1 Gli elementi costitutivi

Chiunque determina altri al suicidio o rafforza l'altrui proposito di suicidio, ovvero ne agevola in qualsiasi modo l'esecuzione, è punito, se il suicidio avviene, con la reclusione da cinque a dodici anni; se il suicidio non avviene, è prevista la reclusione da uno a cinque anni, sempre che dal tentativo di suicidio derivi una lesione personale grave o gravissima.

Quella configurata dall'articolo 580 del codice penale è nella sua sostanza una fattispecie plurisoggettiva necessaria impropria, atteso che alla produzione di uno degli eventi tipizzati dalla norma incriminatrice devono necessariamente concorrere l'azione autolesiva del soggetto passivo (di per sé non punibile) e la condotta del soggetto attivo del reato, che deve risolversi in una forma di istigazione, ossia nella determinazione o nel rafforzamento dell'altrui volontà suicida, ovvero di agevolazione dell'esecuzione del suicidio. Ferma restando l'inapplicabilità delle disposizioni sul concorso di persone nel reato, atteso che la condotta autolesiva del suicida non integra di per sé un illecito penale, il reato è dunque integrato da una partecipazione morale o materiale all'ideazione o esecuzione dell'altrui proposito suicidario<sup>(166)</sup>.

In tal senso la condotta dell'agente, per essere tipica, deve assumere una oggettiva efficienza nella causazione dell'evento del reato<sup>(167)</sup>, la cui produzione deve comunque materialmente rimanere affidata all'azione del soggetto passivo, configurandosi altrimenti le diverse ipotesi di reato di cui agli articoli 575 e 579 del codice penale (omicidio e omicidio del consenziente)<sup>(168)</sup>.

La condotta di partecipazione morale rappresenta dunque, sul piano condizionalistico, un mero antecedente necessario dell'evento, che influisce, sul piano psicologico, sulla determinazione del soggetto passivo di compiere il gesto autolesivo.

In accordo con la dottrina più accorta deve ritenersi, però, che, per risultare tipica, la condotta di partecipazione morale deve presentare un « intrinseco finalismo » orientato all'esito finale, sussistendo altrimenti il rischio di dilatare oltremodo il perimetro oggettivo della

(165) Cass. pen., sez. I, 25 settembre 2020, n. 26862; Cass. pen., sez. V, 24 settembre 2015, n. 43085.

(166) Cass. pen., sez. V, 14 febbraio 2024, n. 17965.

(167) Cass. pen., sez. V, 28 aprile 2010, n. 22782.

(168) E infatti per la legge penale, come sottolineato già nella Relazione al codice penale, il suicidio è un atto volontario compiuto personalmente per procurarsi la morte nella consapevolezza della sua natura autolesiva. Cass. pen., sez. I, 2 febbraio 2023, n. 26015.

fattispecie fino a ricomprendere qualsiasi condotta umana che abbia comunque suscitato o rafforzato l'altrui volontà suicidaria comunque liberamente formatasi.

In tali termini ricostruito, il profilo della condotta tipica si riflette sull'oggetto del dolo necessario per la sussistenza del reato, il quale non solo per questo si tinge dei colori di quello specifico ovvero di quello intenzionale. Va infatti ribadito che quello richiesto dall'articolo 580 è il mero dolo generico, per la cui integrazione è però indispensabile sia la prefigurazione dell'evento come dipendente dalla propria condotta<sup>(169)</sup>, sia la consapevolezza della obiettiva serietà dell'altrui proposito suicida al cui rafforzamento la propria condotta deve per l'appunto concorrere<sup>(170)</sup>.

## 11. L'estorsione sessuale (*sextortion*)

### 11.1 Gli elementi costitutivi

Il termine *sextortion* deriva dall'unione delle parole inglesi « *sex* » (sesso) ed « *extortion* » (estorsione). Si tratta di una operazione delittuosa perpetrata ai danni di utenti internet i quali, con l'illusione di un *flirt* o dell'inizio di una storia sentimentale, inviano proprie immagini o video dal contenuto sessualmente esplicito che vengono, poi, usati come strumento di ricatto.

Solitamente, gli autori di questi reati iniziano a chattare con numerosi utenti in siti specializzati per gli incontri *on line*; una volta carpitata la loro fiducia e acquisite informazioni, invitano le vittime a partecipare ad attività sessuali *on line* che vengono videoregistrate di nascosto. Segue, immediatamente dopo, una richiesta di denaro, accompagnata dalla minaccia di diffondere, in caso di mancato pagamento, il materiale tra tutti i contatti, amici e parenti.

È un fenomeno pericoloso perché fa leva sulla fragilità delle vittime. Spesso le vittime, per timore che le riproduzioni possano essere viste da altri, tendono a non confidarsi con nessuno e a cedere all'intimidazione.

Giuridicamente, la condotta descritta integra il delitto di estorsione: si tratta di un reato particolarmente grave come attestato dalla pena – reclusione da cinque a dieci anni e multa da euro 1.000 a euro 4.000 – che viene comminata a « *chiunque, mediante violenza o minaccia, costringendo taluno a fare o ad omettere qualche cosa, procura a sé o ad altri un ingiusto profitto con altrui danno* ».

Per Matteo Flora, Presidente dell'associazione « PermessoNegato »<sup>(171)</sup>, mentre la pornografia non consensuale (*revenge porn*) colpisce principalmente le donne, la *sextortion*, l'estorsione sessuale, prende di mira gli uomini e viene messa a segno a opera di organizzazioni criminali mosse dall'intento di realizzare un facile profitto. I dati della Polizia postale confermano quelli raccolti dall'associazione: nei mille casi gestiti dal 2020 al 2024, l'80 per cento delle vittime sono uomini.

(169) Cass. pen., sez. V, 28 aprile 2010, n. 22782.

(170) Cass. pen., sez. V, 27 ottobre 2006, n. 3924.

(171) Audizione del 10 novembre 2025.

Si tratta di un crimine di potere, di un abuso che sfrutta le vulnerabilità, di genere, di età<sup>(172)</sup> o psicologiche, per esercitare un controllo o estorcere un profitto.

## 11.2 L'uso di *deepnude*

In tempi più recenti, il fenomeno si è evoluto per effetto dell'impiego delle nuove tecnologie. Le vittime, solitamente personaggi famosi o comunque caratterizzati da una certa notorietà, vengono contattate da sconosciuti che minacciano di diffondere immagini dal contenuto sessualmente esplicito, generate da sistemi di intelligenza artificiale (*deepnude*), se non viene corrisposta una somma di denaro.

Jolanda Renga<sup>(173)</sup>, una delle vittime di questa nuova modalità della *sextortion* che ricorre a immagini artefatte, ha raccontato di aver ricevuto un messaggio, da un numero anonimo, del seguente tenore: « *Pubblicherò a mezzanotte le foto che ho di te nuda. Dì pure ad Ambra* » — il riferimento è alla madre, Ambra Angiolini, attrice e conduttrice televisiva — « *che se non riceverò 10.000 euro ti rovinerò la vita* ». In quell'istante — ha riferito l'audita — « *mi sono sentita senza difese, in imbarazzo di fronte alla parola "nuda", perché il mio corpo è mio e vorrei poter decidere a chi mostrarlo, se e come. In quel momento, però, ho avuto paura che, anche se manipolate, le foto sarebbero state pubblicate e io non avrei potuto farci niente. Mi sono sentita esposta, vulnerabile e colpita nel punto più fragile, la mia dignità, perché c'è sempre una costante, anzi due, che accompagnano la diffusione di queste immagini vere o manipolate: le migliaia di condivisioni sui social e sui gruppi nel privato e i giudizi terribili che scavano dentro di te come persona. La reazione pubblica, infatti, non è quasi mai di empatia, anzi spesso è di scherno, di accusa e di violenza verbale* ».

L'audita ha concluso il suo sofferto racconto spiegando di aver « ... scelto di denunciare ed espormi non per cercare visibilità o compassione, ma ... per chi non ha la mia stessa sicurezza o fortuna nell'aver un rapporto sereno e sano con la propria famiglia, per chi non ha una figura di riferimento di cui si fida e per chi si sente solo e non sa come uscire da una situazione simile e magari sceglie una soluzione estrema per risolvere il problema. A loro spero di trasmettere l'idea che è fondamentale denunciare, perché non esiste vergogna in una richiesta di aiuto e la paura del giudizio non deve vincere ».

(172) Richieste insistenti di denaro per non diffondere sui social immagini « particolari » tali da distruggere la reputazione, un incubo fatto di ricatti ed estorsioni, conosciuto come *sextortion*, si sta diffondendo rapidamente anche tra gli adolescenti. Sono molte le segnalazioni ricevute dalla Polizia postale che interessano ragazzi per lo più tra i 15 e i 17 anni e anche più piccoli: vittime tanto fragili quanto inesperte. Tutto inizia con tentativi di chiacchierata in *chat* da parte di profili *social* di ragazze e ragazzi gentili e avvenenti attraverso gli apprezzamenti e i *like* per le foto pubblicate. Successivamente si passa alla richiesta di immagini e video che con il tempo si fanno sempre più audaci e una volta ottenuti, comincia l'estorsione. Richiesta di soldi, anche piccole somme, per fermare la pubblicazione di contenuti a sfondo sessuale sui social e sulle chat, comprese quelle di genitori, amici e parenti della vittima. Le vittime, intrappolate tra la vergogna e la paura che le immagini intime possano essere viste dai loro contatti, tendono a non confidarsi con nessuno, in particolare con i genitori e per questo motivo si pensa che il fenomeno possa essere sottostimato (<https://www.poliziadistato.it/articolo/sextortion-come-difendersi-i-consigli-della-polizia-postale>).

(173) Audizione del 13 novembre 2025.

## 12. Le lacune

*Rosita Ponticiello*, coordinatrice del Dipartimento Pari opportunità dell'Unione Nazionale Camere Civili <sup>(174)</sup>, ha spiegato che, nel sistema dei *digital crimes*, solo quelli disciplinati dall'articolo 612-ter del codice penale (*revenge porn*) e dall'articolo 612-quater del codice penale (*deepfake*) sono due reati « nativamente » digitali, mentre gli altri reati sono stati estesi alle condotte poste in essere in ambiente o con modalità digitale. È il caso del delitto di atti persecutori, lo *stalking* della diffamazione e della estorsione sessuale.

Manca una legge quadro o, comunque, un insieme di definizioni specifiche ed esclusive per la cyber-violenza di genere, carenza che obbliga a ricorrere all'estensione di reati nati per il contesto fisico, all'interno di un quadro normativo frammentato che genera un'applicazione giudiziaria disomogenea, non esistendo delle fattispecie specifiche che enucleano gli elementi costitutivi dei reati digitali.

Esistono forme di cyber-violenza che oggi non sono assolutamente inquadrare, come il *doxing* con finalità sessista, ovvero la diffusione pubblica di dati personali per esporre la vittima a molestie, difficilmente riconducibile nel reato di atti persecutori, al pari delle cyber-molestie, vale a dire quelle condotte denigratorie o sessiste che vengono reiterate che non sempre generano il grave stato d'ansia o il mutamento delle abitudini di vita della persona offesa.

---

(174) Audizione del 17 novembre 2025.

### Parte III CONSEGUENZE A LIVELLO PSICOLOGICO

#### 1. Il trauma

##### 1.1 La violenza simbolica

La violenza *on line* viene considerata una forma di violenza minoritaria, quasi di serie B, tanto che addirittura gli autori di violenza la minimizzano dicendo che si è trattato di «una sorta di goliardia». Questo perché storicamente l'idea di violenza viene associata al corpo, alla forza fisica, al danno visibile, mentre la violenza digitale agisce attraverso lo spazio simbolico e relazionale con le parole e le immagini, erroneamente considerate meno lesive. Le ferite psicologiche, pur non lasciando lividi, recano tracce profondissime che possono portare non solo a traumi nel lungo periodo ma anche ad ansia, vergogna e isolamento e, nei casi estremi, anche al suicidio.

Come spiegato da *Francesca Schir*, Segretaria del Consiglio nazionale dell'ordine degli psicologi (CNOP)<sup>(175)</sup>, l'illecita pubblicazione su siti sessisti o su pagine *social* di immagini non autorizzate, contraffatte e gravemente offensive della dignità e della riservatezza delle donne che ne sono vittime, ha delle rilevanti ripercussioni di carattere psicologico.

La violenza non è mai solo un comportamento ma diventa, anche nell'ottica e attraverso lo sguardo con cui affrontiamo il tema della violenza *on line*, una relazione patologica di potere che mira a distruggere l'autonomia e l'autostima della persona che ne è vittima. La psicologia riconosce in queste strutture la base di una violenza simbolica e sistemica che prepara il terreno ad atti anche più gravi.

Questa stessa dinamica oggi si è spostata e si è amplificata nello spazio digitale, dove le relazioni si intrecciano con strumenti tecnologici che possono diventare anche mezzi di controllo, sorveglianza, manipolazione o umiliazione pubblica. Ci sono vari strumenti: *cyberstalking*, *revenge porn*, linguaggio d'odio o, addirittura, gruppi digitali che arrivano a disumanizzare la donna divenendo strumenti di violenza psicologica.

La violenza digitale, inoltre, è pervasiva, anonima, senza confini temporali. Non si cancella con un gesto, si diffonde e si moltiplica, per questo ricalca tutte le altre forme di violenza: è una violenza antica, che cambia semplicemente forma, ma non sostanza.

Proprio per questo, il compito della psicologia è quello di riconoscere le nuove forme di questi traumi, le nuove ferite dell'identità e anche le nuove solitudini che ne derivano, perché spesso la reazione è quella del ritiro anche sociale delle donne che spariscono per vergogna, quando la vergogna, ovviamente, dovrebbe accompagnare chi questi atti li compie, non chi li subisce.

I casi di cronaca degli ultimi mesi hanno mostrato con chiarezza quanto la rete possa trasformarsi in uno spazio di oggettivazione, denigrazione e sfruttamento dell'immagine femminile. Non si tratta di episodi isolati, ma sono manifestazioni digitali di quella cultura del

(175) Audizione del 7 ottobre 2025.

possesso e del controllo, in cui corpo e dignità delle donne diventano oggetti di scambio, di derisione.

Dal punto di vista psicologico, questi fenomeni rappresentano una nuova forma di trauma.

Le vittime – ha proseguito l’audita – vivono un dolore permanente, fatto di esposizione, di vergogna, di paura e di perdita di fiducia. Ciò che accade *on line* ha, naturalmente, conseguenze concrete sulla vita reale, sulle relazioni, sul senso di sicurezza, ma anche sulla percezione di sé. È per questo che il contributo della psicologia è unico e insostituibile, perché aiuta a comprendere dinamiche emotive, cognitive e relazionali che alimentano la violenza e, nella fase successiva, a ricostruire il sé nelle vittime.

È assolutamente necessario e importante decostruire stereotipi, linguaggi e rappresentazioni e restituire alle persone strumenti di consapevolezza e di scelta. Nel digitale questa funzione diventa ancora più cruciale perché le persone devono comprendere i meccanismi psicologici della manipolazione *on line* e quelli della vergogna e del senso di colpa che spesso bloccano le vittime.

## 1.2 Le carenze

Manca una formazione specifica sotto il profilo della competenza psicologica. Non si ha contezza dell’impatto sulla psiche della violenza *on line*, come a volte ci raccontano vittime che, in sede di denuncia, non si sentono comprese perché è difficile valutare il trauma derivante dall’esposizione mediatica. Questo naturalmente crea una forma ulteriore di aggravamento della situazione. In più, il contesto virtuale viene percepito come meno reale, anche se il cervello reagisce alle violenze digitali come a quelle fisiche attivando gli stessi circuiti di stress e di paura.

Si registra, inoltre, una scarsa comunicazione interistituzionale.

Una collaborazione fra psicologi, magistrati, assistenti sociali e Forze dell’ordine in *team* multidisciplinari potrebbe essere utile ove venisse formalizzata e resa strutturale. Questo potrebbe generare dei circoli virtuosi che potrebbero portare a valide forme di collaborazione e non a distorsioni che poi generano ritardi nella protezione, misure contraddittorie o frammentazioni nel percorso che riguarda sia le vittime sia gli autori delle violenze *on line*.

## 1.3 Le azioni concrete proposte dal Consiglio nazionale dell’ordine degli psicologi (CNOP) nella prevenzione della violenza digitale

Il Consiglio nazionale dell’ordine degli psicologi (CNOP), anche attraverso il Comitato delle Pari opportunità, nel Quaderno « *Contrasto alla violenza di genere* », ha indicato una serie di azioni concrete e alcune linee operative per affrontare le nuove forme di violenza nello spazio digitale. Tra queste spicca l’educazione al consenso e alla cittadinanza digitale consapevole, tramite la promozione di percorsi

educativi che aiutino le nuove generazioni a riconoscere e a prevenire tutte le situazioni di abuso e di manipolazione *on line* <sup>(176)</sup>.

Il riconoscimento precoce delle forme emergenti di violenza digitale si attua attraverso la formazione dei professionisti sul *cyberstalking*, sul *sexting*, sul *revenge porn*, sull'*hate speech*, con linee guida condivise, nonché con campagne di sensibilizzazione e formazione permanente su questo tema in collaborazione con i *media* e le istituzioni <sup>(177)</sup>.

Un tema veramente importante riguarda il ruolo dei modelli familiari e il sostegno alla genitorialità: il contrasto alla violenza, anche digitale, non può essere demandato solo alla scuola, quando i modelli relazionali in qualche modo sono già consolidati ma deve partire dai modelli familiari e genitoriali, dalle prime relazioni di cura, da ciò che i bambini apprendono osservando come gli adulti si parlano e si rispettano. È nella primissima infanzia che si forma questa capacità di riconoscere l'altro come soggetto e non come oggetto.

Per questo il CNOP ha proposto di rafforzare la rete di supporto psicologico alla genitorialità e alla prenatalità, valorizzando i consulenti, i servizi 0-6 e i punti nascita anche come luoghi di prevenzione della violenza.

La promozione della salute psicologica e genitoriale è una misura di prevenzione primaria: aiuta a interrompere questa trasmissione intergenerazionale della violenza e a favorire le relazioni sane, basate su empatia e reciprocità. Le relazioni sane devono essere basate su questi due aspetti, perché diventano centrali nella trasmissione di modelli funzionali. Educare alla relazione non può essere un compito da delegare solo alla scuola: è una responsabilità collettiva e la psicologia può offrire sicuramente un contributo strategico ma soprattutto scientifico e anche umano.

La violenza di genere *on line* è una nuova frontiera della violenza, una violenza invisibile ma devastante, perché colpisce l'identità, la reputazione e la percezione di sé, il che naturalmente genera traumi

(176) Oggi la violenza di genere viene spesso raccontata come un'emergenza, ma non lo è. È un fenomeno strutturale, radicato nella nostra cultura, nei linguaggi, nei modelli di relazione, negli stereotipi che continuiamo a tramandare. Non nasce all'improvviso, non è un *raptus*, ma cresce lentamente in una società che troppo spesso giustifica, minimizza o resta in silenzio. L'educazione è l'unica risposta sistematica possibile. Non possiamo delegare ai tribunali ciò che spetta alla scuola, alla famiglia, alle istituzioni culturali. È lì, nelle aule e nei luoghi di formazione, che possiamo insegnare ai nostri ragazzi a riconoscere la violenza prima che si trasformi in gesto, prima che diventi tragedia (così Gino Cecchetti, Presidente della Fondazione Giulia Cecchetti, audizione dell'11 novembre 2025).

(177) Silvia Semenzin, nel corso dell'audizione del 16 ottobre 2025, ha segnalato che è in preparazione da parte del Consiglio d'Europa un corso gratuito che sarà disponibile per tutti gli esperti professionali legali per formarsi sulla violenza di genere *on line*. Secondo l'audita «Sarebbe utile renderlo obbligatorio anche in Italia, perché questo aiuterebbe a superare una serie di limiti che oggi le vittime hanno nel momento in cui si trovano a voler denunciare e si ritrovano a essere rivittimizzate sia nei processi giudiziari che nei procedimenti di polizia. Questo non sempre garantisce un trattamento rispettoso delle vittime. Si può anche promuovere la creazione di sezioni specializzate o task force interdisciplinari sulla violenza di genere *on line*, oltre a un supporto alle attuali reti antiviolenza che sono le uniche che al momento stanno fornendo aiuto alle donne che effettivamente si ritrovano all'interno di questi processi. Proporrei anche l'istituzione di un osservatorio pubblico sulla violenza di genere *on line*, che al momento non abbiamo, ma che sarebbe particolarmente importante per garantire: un monitoraggio costante dei fenomeni emergenti, la raccolta dati e gli indicatori comparabili a livello europeo, come viene richiesto dalla direttiva europea sulla violenza domestica».

enormi che possono condurre, soprattutto nelle giovani generazioni, anche a decisioni fatali. Ma può essere contrastata attraverso conoscenza, prevenzione e cambiamento culturale.

La psicologia può offrire una chiave di trasformazione profonda, sia individuale che collettiva, attraverso la cultura della relazione, del rispetto e della responsabilità anche nello spazio digitale.

## Parte IV LA TUTELA OFFERTA DALLE PIATTAFORME

### 1. Le segnalazioni

#### 1.1 Le criticità

Per *Elisabetta Fersini*, professoressa associata di informatica presso l'Università degli Studi di Milano Bicocca<sup>(178)</sup>, la violenza di genere *on line* può assumere diverse forme che possono variare sulle varie piattaforme per linguaggio e modalità di comunicazione. All'interno delle piattaforme *on line*, tipicamente le piattaforme sociali, sono in continua crescita contenuti di varia forma: messaggi, commenti, immagini esplicite, video e in alcuni casi anche audio.

All'interno di queste piattaforme, le forme di molestia, le forme di discriminazione e di sessismo sono disponibili quotidianamente<sup>(179)</sup>. Le piattaforme hanno attivato meccanismi di segnalazione, tuttavia, non sempre idonei a contenere e rimuovere contenuti espressivi di forme di odio, in particolare contro le donne<sup>(180)</sup>.

Il c.d. *Digital Services Act* (DSA, Regolamento 2022/2065/UE del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che

(178) Audizione del 15 ottobre 2025.

(179) Osserva *Lilia Giugni*, professoressa di Innovazione inclusiva presso l'*University College* di Londra e ricercatrice di Innovazione sociale presso l'Università di Cambridge (audizione del 17 novembre 2025), che nel nostro Paese, come in molti altri, gli interventi legislativi sulla violenza digitale si sono concentrati finora principalmente sul piano delle condotte individuali, cioè quello di chi commette atti violenti facilitati dalla tecnologia, ad esempio minacciando una donna via *social* o violando la sua intimità *on line*. Chiaramente ci si è avvalsi a questo scopo dello strumento penalistico. Però, è evidente che purtroppo in questo caso le condotte individuali non sono che la punta dell'*iceberg*, come si suol dire. Questo perché dietro ai comportamenti dei singoli utenti si cela un apparato di attori tecnologici ed economici di piattaforme che facilitano la violenza digitale e che spesso, direttamente o indirettamente, ne traggono profitto.

(180) Per *Laura Bononcini*, *Public Policy Director* di Meta per il Sud-Europa, la segnalazione degli utenti è assolutamente fondamentale. «Un utente può segnalare qualsiasi tipo di contenuto su Meta, quindi su Facebook, su Instagram, eccetera, che si tratti di un post, di un'immagine o di un intero account. Utilizziamo, inoltre, per identificare i contenuti potenzialmente in violazione, l'intelligenza artificiale. In alcuni casi, anzi nella maggior parte dei casi, l'intelligenza artificiale è in grado di identificare e di rimuovere automaticamente una quantità molto importante di contenuti in violazione delle nostre policy. Utilizziamo l'intelligenza artificiale anche per far emergere, innanzitutto, le segnalazioni degli utenti oppure i contenuti che vengono individuati dalla stessa intelligenza artificiale che necessitano di una revisione umana. Ci tengo a sottolineare che non tutti i contenuti contrari alle nostre policy possono essere individuati dall'intelligenza artificiale: in molti casi c'è bisogno di un'analisi di contesto, di comprensione del contenuto stesso, soprattutto se parliamo di contenuti scritti, quindi il ruolo dei revisori che si occupano di rivedere questi contenuti è fondamentale. Abbiamo migliaia di revisori in tutto il mondo, attivi 24 ore su 24. Potete trovare più informazioni sulla natura e anche sulla quantità dei contenuti rimossi e come vengono identificati e rimossi sul nostro report di trasparenza, che pubblichiamo regolarmente. Tra aprile e giugno del 2025 siamo intervenuti su 9,6 milioni di contenuti che mostravano nudità e attività sessuali di adulti; il 96,4 per cento di questi contenuti è stato rimosso automaticamente, senza nemmeno che gli utenti lo dovessero segnalare. È fondamentale la segnalazione, nel senso che veramente è molto importante rendersi conto che qualsiasi contenuto segnalato viene rivisto o tramite l'intelligenza artificiale o direttamente dai nostri revisori. A seguito della segnalazione ci sarà un'azione o meno se pensiamo che non ci sia una violazione delle nostre policy. È chiaro che nel caso in cui il contenuto non violi le policy di Meta, ma violi la legge italiana, è probabile che la denuncia sia più efficace anche perché in quel caso, come dicevo prima, la procedura sarebbe diversa, quindi è l'autorità che ci segnalerà il contenuto e noi procederemo col blocco» (audizione del 27 novembre 2025).

modifica la Direttiva 2000/31/CE dell'8 maggio 2001) è il regolamento europeo sui servizi digitali che prevede obblighi proporzionati alla dimensione della piattaforma e una nuova cultura della prevenzione dei rischi sistemici, dalla disinformazione ai contenuti illegali <sup>(181)</sup>.

Le statistiche dimostrano che, per quanto riguarda soprattutto il contesto delle lingue minoritarie (tra cui l'italiano), nelle piattaforme vi è un numero di moderatori molto inferiore rispetto a lingue quali l'inglese, il francese e il tedesco: ne è un esempio il caso del gruppo *Facebook* « Mia moglie » in cui è emerso che, già in passato, vi erano state molte segnalazioni prese in carico solo dopo il mese di agosto 2025.

Nella memoria fatta pervenire dall'ingegnere *Paolo Reale* <sup>(182)</sup>, gli attuali sistemi di segnalazione offerti dalle piattaforme risultano spesso inefficaci e frustranti.

Le risposte a seguito di segnalazione sono praticamente sempre negative (« *il contenuto non viola le nostre policy* »). « *È possibile proporre ricorso avverso questa decisione, ma dopo aver ulteriormente spiegato le ragioni della segnalazione, e del ricorso stesso, questo si interrompe dopo la "presa in carico", senza che vi siano più risposte in merito, e comunque nella totale assenza di motivazioni puntuali e specifiche. Il paradosso è che chi segnala deve fornire i propri dati e motivare la richiesta, quindi facendosi riconoscere, mentre chi diffonde odio o diffamazione può restare anonimo e invisibile, e non è neppure tenuto a rispondere a chi ha operato la segnalazione. In alcuni casi, addirittura, la segnalazione ha seguito un iter di richiesta di sempre migliori specifiche arrivando a 5-6 mail senza che neppure venisse avviato il meccanismo di verifica. In altri casi, il provider si rifiuta di fornire alcuna risposta al segnalatore, spiegando che il reclamo viene gestito direttamente con il segnalato, in evidente violazione del DSA* » <sup>(183)</sup>.

## 1.2 I rimedi

Le piattaforme, tecnicamente parlando, permettono di accedere legittimamente a contenuti, immagini, commenti che possono essere potenzialmente discriminatori, misogini o sessisti <sup>(184)</sup>.

(181) L'articolo 16 (Meccanismo di segnalazione e azione) del DSA prevede che « *1. I prestatori di servizi di memorizzazione di informazioni predispongono meccanismi per consentire a qualsiasi persona o ente di notificare loro la presenza nel loro servizio di informazioni specifiche che tale persona o ente ritiene costituiscano contenuti illegali. Tali meccanismi sono di facile accesso e uso e consentono la presentazione di segnalazioni esclusivamente per via elettronica* ».

(182) In data 7 ottobre 2025.

(183) Nel corso dell'audizione del 7 ottobre 2025, l'ing. Reale ha sostenuto che « *sicuramente occorre tenere conto di una serie di procedure e regolamenti europei che devono essere armonizzati e che oggi consentono di avere degli strumenti potenti: il Digital Services Act, la direttiva e il regolamento E-Evidence sono due strumenti effettivamente che, se attuati in modo corretto, possono essere potentissimi. Sicuramente l'AGCOM, che è l'organismo che si deve far carico del rispetto di questo, se rafforzato opportunamente, se introduce correttamente meccanismi di monitoraggio e controllo e anche delle procedure disponibili al cittadino, può essere uno strumento efficace in questa fase; così come anche valutare la possibilità di introdurre delle modalità di anonimato che per alcuni soggetti e per alcune situazioni, laddove soprattutto ci sono molti iscritti e molti follower, probabilmente porta ad avere un approccio legato alla responsabilità* ».

(184) Sono stati varati sistemi a tutela del diritto d'autore, ad esempio « *Piracy Shield* », per evitare la diffusione di trasmissioni pirata che sono attive già in questo momento, che fanno in modo che, a fronte di una segnalazione giunta all'ISP (*Internet Service*

Sono due le modalità di accesso a queste piattaforme.

Tra le modalità ufficiali ritroviamo quelle che, in gergo, vengono chiamate le API (*Application Programming Interface*) ufficiali. Alcune piattaforme offrono la possibilità di accedere direttamente dal proprio computer a contenuti sessisti o misogini. Esistono poi altre vie, vietate, tra cui il *crawler* e lo *scraping*. Mentre nel primo caso è possibile accedere a contenuti pubblici o autorizzati, per cui esiste un'esplicita dichiarazione di contenuto pubblico o di autorizzazione alla concessione del dato, nel caso in cui i contenuti non siano pubblici o autorizzati, tecnicamente è possibile accedere, ma legalmente è vietato dai termini di sicurezza delle piattaforme che possono incorrere in potenziali violazioni del GDPR (*General Data Protection Regulation*).

Il *Digital Service Act* viene incontro in questa direzione, consentendo l'accesso ai ricercatori e alle Forze dell'ordine.

Per contrastare il fenomeno della violenza nella sfera digitale, il primo passo fondamentale è il monitoraggio che può avvenire con una ricerca manuale sulle piattaforme chiuse, eventualmente anche a fronte di segnalazione, oppure con una ricerca automatica sulle piattaforme aperte<sup>(185)</sup>. Questo perché ci sono stati casi pregressi – di cui tra l'altro anche il gruppo *Facebook* « Mia moglie » ha dato evidenza –, per cui i contenuti, che tipicamente vengono raccolti e pubblicati all'interno di queste piattaforme, non seguono un unico canale di comunicazione, ma vengono in realtà poi suddivisi su molteplici canali, alcuni dei quali aperti, per cui facilmente accessibili o parzialmente accessibili anche per mezzo di ricerche automatiche, con l'ausilio di strumenti di ricerca e quindi della tecnologia.

Oltre a questo primo passaggio, in cui la ricerca manuale si affianca a quella automatica – quindi sia su piattaforme chiuse che su quelle aperte –, per contrastare il fenomeno della violenza digitale si fa ricorso a strumenti di « *reverse image search* », come *Google* immagini o *TinEye*, che permettono di trovare copie di immagini che sono

---

*Provider*) quest'ultimo debba sospendere l'accesso a quel portale, a quel sito che trasmette i contenuti pirata in tempi estremamente ridotti (si parla di mezz'ora o un'ora a seconda delle situazioni). Per le segnalazioni che, invece, riguardano qualcosa che va a impattare sulla *privacy* delle persone – anche su contenuti estremamente sensibili e delicati come i temi sessuali – non esiste un meccanismo analogo, per cui anche le autorità di polizia devono procedere con metodologie che sono necessariamente più lunghe e che richiedono più tempo (*Diego Marson, Chief Technical Officer* di *Yarix Var Group*, audizione del 17 novembre 2025).

(185) Come spiegato da Laura Bononcini, *Public Policy Director* di Meta per il Sud-Europa, nel corso della audizione del 27 novembre 2025, Meta è stata « la prima azienda ad avere l'intuizione di utilizzare le tecnologie di riconoscimento delle immagini per finalità di rimozione di contenuti di NCII, quindi la condivisione non consensuale di immagini intime. L'idea è nata con la creazione da parte di Meta, che poi ha coinvolto oltre cento associazioni e praticamente tutti gli altri operatori del settore, della piattaforma "StopNCII". Questa piattaforma consente agli utenti che hanno paura che una loro immagine venga condivisa sulle piattaforme on line di applicarvi una sorta di impronta digitale, in modo che questa impronta digitale possa essere utilizzata dai sistemi tecnologici di tutte le aziende Meta, ma anche i vari social network internazionali, americani, europei, eccetera, per rimuovere automaticamente questi contenuti. Questo è uno strumento che si può utilizzare, di cui viene incoraggiato l'utilizzo, anche se si ha paura che questa tipologia di contenuti potrebbero essere condivisi. Quindi, anche se non si sa se sono stati o meno condivisi, questi strumenti consentono di rimuovere automaticamente questi contenuti o contenuti simili. Abbiamo lanciato anche la piattaforma "Take it Down". La piattaforma "StopNCII" è dedicata agli adulti, mentre "Take it Down" è dedicata ai ragazzi al di sotto dei 18 anni. È importante sottolineare che "Take it Down" e "StopNCII" funzionano anche con i contenuti generati dall'AI ».

state condivise. Una volta acquisite le immagini potenzialmente misogine, sessiste o che, in generale, possono avere contenuti inopportuni, questi strumenti, alla portata di tutti, permettono di tracciare la diffusione e individuare ulteriori gruppi e pagine che ospitano contenuti analoghi. Oltre a questo, è possibile monitorare delle piattaforme alternative, quali *Telegram* e *Discord*, dove spesso si ricollocano i contenuti rimossi dalle piattaforme chiuse. In questo caso è possibile accedervi per vie ufficiali, attraverso quelli che, in gergo, vengono chiamati « *client* » o « *bot* » inseriti all'interno di *chat* e canali pubblici.

Per contrastare i fenomeni di violenza di genere *on line*, inoltre, sono disponibili diversi strumenti di intelligenza artificiale.

*Google*, *Amazon* e *Microsoft* forniscono dei servizi – anche non a pagamento – che offrono funzionalità per rilevare contenuti quali nudità, contenuti sessualmente espliciti e solitamente vengono utilizzati come un « macro filtro » per effettuare una prima rilevazione dei fenomeni macroscopici. Oltre agli strumenti commerciali, esistono anche degli algoritmi, dei modelli di intelligenza artificiale che sono stati definiti nel corso degli ultimi anni al fine specifico di riconoscere le potenziali forme di violenza di genere.

### 1.2.1 I modelli di visione e di linguaggio e gli algoritmi

I sistemi di intelligenza artificiale possono utilizzare diverse tipologie di modelli: quelli di visione, che si basano sull'analisi delle singole immagini, essendo addestrati per identificare la tipologia del contenuto, come, ad esempio, la presenza di soggetti specifici, o a distinguere la sessualizzazione consensuale da quella non consensuale; quelli di linguaggio, che, invece, analizzano il contenuto testuale tipicamente associato ai commenti. Questi ultimi modelli vengono formati sulla specificità del linguaggio misogino che ha delle caratteristiche molto particolari.

I modelli di visione e di linguaggio sono delle reti neurali artificiali molto complesse, preaddestrate o adattate per contenuti eventualmente misogini o sessisti che integrano i meccanismi di ragionamento impiegati per la ricerca dei contenuti testuali e visuali.

Gli strumenti automatici sono di forte ausilio ma non sono sufficienti per completare il percorso di riconoscimento; occorrono anche gli strumenti « *explainability* », ovvero di spiegabilità del motivo per cui un algoritmo di intelligenza artificiale ha rilevato un determinato contenuto sessista o di altro tipo. Non essendo infallibili, gli algoritmi possono dare indicazioni sbagliate ma, fortunatamente, in eccesso, con indicazione di falsi negativi essendo in grado di cogliere tutti i contenuti misogini e sessisti.

Gli algoritmi possono essere perfezionati con la supervisione dell'essere umano che da una parte può svolgere una funzione fondamentale di verifica di quella che è la decisione dell'algoritmo, dall'altra può produrre raccomandazioni e *feedback* da includere all'interno dei meccanismi di revisione degli algoritmi di intelligenza artificiale.

La copertura dei modelli di intelligenza artificiale ad oggi disponibili è molto buona per i sistemi di lingua inglese, esistendo strumenti in grado di riconoscere contenuti sessisti, violenti o abusivi in una

percentuale davvero elevata; per l'italiano è di poco inferiore ma in crescita <sup>(186)</sup>.

La difficoltà maggiore è collegata al rilevamento delle c.d. forme implicite.

Mentre è abbastanza semplice individuare una forma di sessualizzazione, un contenuto misogino chiaramente esplicito – quale, ad esempio, un inno alla violenza contro il genere femminile –, diventa molto complesso ravvisare le c.d. forme implicite, in cui non c'è un'indicazione semanticamente chiara del contenuto.

Occorre raccogliere dati e creare dei banchi di prova per migliorare la copertura linguistica, affiancando alla ricerca umana strumenti automatici che effettuano un *pre-screening* anche ricorrendo a sistemi che raccolgono i dati in modo semiautomatico.

La ricerca si indirizza verso la creazione di risorse condivisibili, rispettando tutti i perimetri del GDPR e delle normative europee, per creare *benchmark* di valutazione con una doppia funzione: da una parte, istruire gli algoritmi di intelligenza artificiale, dall'altra, metterli a regime e valutare quanto siano effettivamente accurati in contesti sempre più complessi.

Un'altra sfida, nel panorama non solo italiano, è l'individuazione del *bias*.

Gli algoritmi e i modelli di intelligenza artificiale possono essere in qualche modo condizionati dagli esempi che noi forniamo a questi strumenti per cercare di insegnare cosa è un contenuto sessista, misogino o abusivo, finendo con il trasmettere al programma il pregiudizio di chi è portatore, anche inconsapevolmente, chi lo addestra.

I campioni raccolti possono prediligere una certa popolazione, quindi immaginiamo un linguaggio in cui si associa spesso alla parola « donna » l'appartenenza al luogo domestico: questa associazione e questa correlazione spuria, nel momento in cui si riverbera all'interno dei dati, porta inevitabilmente i modelli a effettuare delle previsioni che possono generare falsi positivi. In questo caso, da un punto di vista scientifico, ci sono delle strategie computazionali che possono essere adottate per contenere il problema.

Il lavoro più complicato rimane quello della individuazione delle c.d. forme implicite: i modelli ad oggi disponibili, nonostante siano sempre più istruiti e abbiano sempre più dati a disposizione per riconoscere le forme di violenza di genere *on line*, ancora faticano a riconoscere le forme sottili, concettualmente molto articolate in cui il confine con le forme di odio *on line* risulta molto labile.

L'unica soluzione, allo stato, è una continua revisione da parte dell'essere umano con costante aggiornamento dei modelli in quel momento storico disponibili.

### 1.2.2 I « *trusted flaggers* » (i segnalatori attendibili)

Il *Digital Services Act* (DSA) ha introdotto la figura dei *trusted flaggers* (articolo 22), soggetti qualificati che segnalano contenuti illegali

(186) Sulla base di test « di laboratorio » è emerso che la ricerca in lingua inglese ha una maggiore percentuale di successo (ci aggiriamo intorno al 90 per cento). In lingua italiana, con gli strumenti ad oggi disponibili, per quanto riguarda contenuti meramente testuali ma anche contenuti sia testuali che visuali (immagini, *meme* e contenuti audio), è di poco inferiore (circa l'85 per cento).

alle piattaforme *on line* con una corsia preferenziale per la loro rimozione, designati dalle autorità competenti degli Stati membri – nel caso italiano dall'AGCOM – sulla scorta di criteri stringenti di competenza e indipendenza.

Un segnalatore attendibile deve operare in settori specifici, come la protezione dei diritti d'autore, la lotta alla disinformazione, il contrasto alle frodi e alle truffe *on line*, all'incitamento all'odio e allo sfruttamento sessuale.

Le piattaforme digitali, in particolare le *Very Large Online Platforms* (VLOP) e i *Very Large Online Search Engines* (VLOSE), sono tenute a trattare le segnalazioni di questi soggetti con priorità e con maggiore attenzione rispetto a quelle provenienti da utenti ordinari.

Matteo Flora, Presidente dell'associazione PermessoNegato<sup>(187)</sup>, ha evidenziato che le piattaforme lavorano a due livelli: nel primo livello, la piattaforma « valida » i contenuti per vedere se la segnalazione è corretta; nel secondo livello, i segnalatori, tramite degli *account* speciali che entrano in aree dedicate dei singoli portali o delle mail di riferimento, una volta riscontrata la natura non consensuale del contenuto, ne consentono la rimozione.

Ogni piattaforma ha una diversa modalità operativa: una, in particolare, che si occupa di siti pornografici, quando arriva la segnalazione, ancora prima di verificarla, rimuove il contenuto *on line*.

Negli ultimi anni si è assistito ad un miglioramento della risposta da parte delle piattaforme che danno sempre maggiore importanza alle segnalazioni. Residuano errori e ritardi ma in numero più contenuto rispetto al passato. Purtroppo, alcune piattaforme non considerano le segnalazioni perché non hanno interesse a rimuovere il contenuto<sup>(188)</sup> oppure non sono incluse, come nel caso di *Telegram*. In quel caso occorre individuare lo Stato competente, dove si trova, ad esempio, il *server* o il fornitore del servizio, e attivare la *authority* di riferimento.

### 1.3 L'esperienza « Meta »

Claudia Trivilino, *Public Policy Manager* di Meta per Italia e Grecia<sup>(189)</sup>, ha spiegato che, per quanto riguarda la condivisione dei dati con le Forze dell'ordine e la magistratura, l'approccio dell'azienda è sempre a più livelli, considerato il carattere transfrontaliero della rete. Ogni *team* nazionale ha esperti di *public policy*, di *law enforcement* e *law enforcement outreach*, quindi persone che si occupano di fare questo lavoro con le Forze dell'ordine o la magistratura e che coadiuvano le richieste su condotte integranti un reato che vengono acquisite attraverso canali dedicati e gestite, in conformità agli accordi internazionali, sulla base del principio di buona fede.

(187) Audizione del 10 novembre 2025.

(188) Talvolta la piattaforma ha interesse a mantenere contenuti « polarizzanti » che fanno visualizzazioni e che, in virtù di meccanismi algoritmici, vengono rilanciato normalizzando le violenze digitali, come dichiarato da Mariacristina Sciannamblo, professoressa associata di sociologia e scienze sociali applicate e coordinatrice del progetto GIVRE – *Gendering Internet. Violence, Resilience and Empowerment in digital spaces* (2023-25), nel corso dell'audizione del 12 febbraio 2026. L'audita ha anche affermato di aver registrato, nel corso delle numerose interviste qualitative effettuate, un grande scetticismo sull'efficacia della segnalazione da parte delle vittime.

(189) Audizione del 27 novembre 2025.

Per quanto riguarda poi le procedure ordinarie, l'azienda fa sempre riferimento al *Mutual legal assistance treaty*, un accordo internazionale che impegna le piattaforme a condividere, attraverso una rogatoria, i dati in presenza di una procedura nazionale riconosciuta come legittima. Di grande importanza è il pacchetto *E-evidence* (Regolamento 2023/1543/UE e Direttiva 2023/1544/UE del 12 luglio 2023) che ha modificato le procedure relative alle richieste di informazioni attraverso ordini di preservazione del contenuto e condivisione dei dati, creando una procedura semplificata europea, senza necessità di rogatoria internazionale, garantendo, così, un regime di obbligatorietà della condivisione di contenuti.

Per *e-evidence* si intendono le prove elettroniche, ossia dati digitali, come email, messaggi, *file*, contenuti multimediali, conservati su dispositivi informatici e utilizzati come prove in processi, anche penali: in pratica, ogni dato generato, trasmesso, trattato o conservato da computer o altri dispositivi informatici.

Vi rientrano non solo i *file* – come messaggi, video, audio, foto – ma anche i dati conservati dai fornitori di servizi (*service providers*) (per esempio i c.d. « dati di traffico ») con riferimento ai flussi informativi in transito nella rete o nei dispositivi, oggetto di captazione in tempo reale.

Il regolamento comunitario disciplina la circolazione transnazionale delle prove elettroniche, ossia tra procure e uffici giudiziari dei Paesi UE. Destinato a entrare in vigore nel luglio 2026, introduce una svolta epocale: disciplina gli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive, configurando un sistema che supera i tradizionali canali di cooperazione giudiziaria tra Stati membri<sup>(190)</sup>. La vera novità consiste nel fatto che, per ottenere dati detenuti da un prestatore di servizi stabilito in un altro Stato membro, non sarà più necessario il coinvolgimento delle autorità giudiziarie dello Stato di esecuzione. In forza del principio del mutuo riconoscimento, e nel rispetto di specifiche condizioni (nonché laddove una simile misura sia ammessa in casi interni analoghi), le autorità competenti – che non devono essere necessariamente giudiziarie – potranno rivolgersi direttamente al prestatore di servizi straniero, ordinando la produzione o la conservazione, entro termini prestabiliti, di dati di abbonato, dati relativi al traffico e persino dati di contenuto.

#### 1.4 L'attuazione della Direttiva *E-evidence*

La Direttiva 2023/1544/UE, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali, è stata recepita nel nostro Paese con il decreto legislativo 30 dicembre 2025, n. 216.

(190) Nell'era digitale, ha calcolato il Consiglio Ue, l'85% delle indagini penali fa ricorso ai dati digitali. E in oltre il 50% di tutte le indagini penali si effettuano richieste transfrontaliere finalizzate all'ottenimento di prove elettroniche.

## 2. L'anonimato on line

### 2.1 La celere identificazione del responsabile

Nel corso dell'audizione del 16 ottobre 2025, *Marisa Marraffino* – avvocatessa penalista esperta di diritto dell'informatica, tutela della reputazione aziendale e dei privati nei *new media* e per la gestione della *privacy* – ha ricordato che i *social network* sono tornati, anche in Italia, sotto l'ombrello della Direttiva 2000/31/CE, nota anche come direttiva sul commercio elettronico, recepita nel nostro Paese con il decreto legislativo 9 aprile 2003, n. 70. In particolare, l'articolo 3, comma 2, della direttiva ha stabilito chiaramente che gli Stati membri non possono limitare la libera circolazione dei servizi della società dell'informazione. Sono previste, però, anche delle deroghe: il quarto comma dell'articolo 3 prevede che per particolari ragioni – tra le quali rientra l'esigenza di tutela e di lotta contro i reati contro l'incitamento all'odio e di discriminazione sessuale – gli Stati membri possano intervenire.

Secondo l'audita, quest'ultima previsione consentirebbe al nostro Paese l'adozione di tutele più efficaci alle vittime.

Una prima proposta di riforma potrebbe essere quella di rendere più efficace l'identificazione degli utenti che attualmente operano nel più completo anonimato<sup>(191)</sup>.

In Italia vi sono difficoltà tecniche anche nella identificazione di chi banalmente usa un « *nickname* ».

Questo non significa compromettere la *privacy* degli utenti: la riservatezza è un diritto che può essere bilanciato con altri diritti di pari grado, in questo caso quello della sicurezza degli utenti della rete.

L'individuazione immediata del responsabile avrebbe una funzione deterrente nei confronti di soggetti che attualmente pensano di poter operare impunemente e, soprattutto, indurrebbe le vittime – donne, che sono le più colpite dalla violenza digitale – a querelare superando l'idea che « *tanto non succede niente, tanto nessuno riuscirà a identificare chi c'è dietro ed è impossibile arrivare a identificare i responsabili* »<sup>(192)</sup>.

(191) *Claudia Trivilino, Public Policy Manager di Meta per Italia e Grecia*, nel corso della audizione del 27 novembre 2025, ha dichiarato che l'azienda chiede, su tutte le piattaforme, che gli utenti siano autentici: « *il principio che seguiamo è l'autenticità, cioè l'identificazione della persona, la trasparenza rispetto a chi si è. Infatti, su Facebook c'è proprio la richiesta, attraverso le nostre policy, di autenticità del soggetto, posto che per quanto riguarda la presenza degli individui on line torna quel bilanciamento di interessi che abbiamo discusso. Dobbiamo bilanciare l'obbligo di identificarsi con la possibilità di potersi esprimere pienamente per ciò che si è all'interno delle piattaforme* ». L'audita ha tuttavia osservato che « *Richiedere l'identificazione attraverso, ad esempio, la condivisione della carta d'identità o dei dati di identità intanto confligge con i principi base di minimizzazione dei dati ed è un controsenso rispetto al principio di minimizzazione del dato, e della sua condivisione con aziende private, che poi è la richiesta in generale che la società fa. Ciò mette in grave difficoltà o in una posizione più difficile coloro che hanno, ad esempio, limitate disponibilità ad avere una carta d'identità o un'identità certificata, perché se noi permettessimo l'accesso di soggetti alle piattaforme su identificazione con la carta d'identità dovremmo lasciare fuori chi la carta d'identità, ad esempio per ragioni nazionali, non ce l'ha, oppure l'obbligo di identificazione del soggetto, di soggetti che sono survivor di reati, whistleblower, la cui identità deve essere nascosta o si deve mantenere nascosta. La posizione di questi soggetti potrebbe essere penalizzata da un obbligo di questo tipo* ».

(192) Per quanto riguarda un intervento tecnico nell'immediato, l'ing. Reale, nel corso della sua audizione del 7 ottobre 2025, ha suggerito « *di rendere sempre più agevole e*

Alle piattaforme – ha concluso l’audita – dovrebbero essere date massimo 48 ore per fornire i dati richiesti in presenza di un fatto di reato; adesso, con l’identificazione a due fattori, le piattaforme dispongono di una miriade di dati personali tali da consentire l’immediata identificazione dell’utente <sup>(193)</sup>.

### 3. La rimozione immediata dei contenuti

#### 3.1 La crittografia

Il più grave *vulnus* nel sistema nella tutela delle vittime dei reati *on line* è rappresentato dalla difficoltà di ottenere la rimozione immediata dei contenuti.

Quando un contenuto diventa virale – e quello a sfondo sessuale lo diventa in maniera molto rapida (possono raggiungere anche 2-3 milioni di visualizzazioni) – le vittime si sentono impotenti, consapevoli dell’impossibilità di far rimuovere l’immagine o il video diffuso in rete.

A impedire un intervento tempestivo è la crittografia <sup>(194)</sup> di molte piattaforme perché – al di là dei *social* principali che, in presenza di reati particolarmente gravi, collaborano con l’autorità giudiziaria – ne esistono tantissime, come si è scoperto con il caso dei « siti sessisti », che non consentono la visualizzazione e rimozione <sup>(195)</sup>.

### 4. La scansione delle immagini

#### 4.1 La pseudonimizzazione tramite il codice *hash*

Una forma di tutela preventiva è rappresentata dalla scansione delle immagini o dei video che consente, grazie alla collaborazione dei

---

*sempre più facile l’accesso alle informazioni indispensabili per il riconoscimento. Questo significa che siccome oggi si passa sempre attraverso la rogatoria internazionale – la maggior parte delle piattaforme stanno tutte al di fuori dell’Unione europea – in tutti i casi praticamente bisogna chiederle fuori. Questo comporta dei tempi di risposta che sono oggettivamente lunghissimi. Stiamo parlando di diversi mesi, in alcuni casi si può arrivare a otto-dieci mesi semplicemente per avere delle risposte. Forse l’intervento tecnico che può aiutare è un’adozione ancora prima del suo arrivo come direttiva europea e regolamento dell’E-Evidence, visto che già comincia a indirizzare, costringe ad avere un rappresentante legale nella nazione. Quindi, la richiesta si può fare all’interno della nazione senza la rogatoria, imponendo dei tempi di risposta che siano accettabili per le indagini. Attualmente, la conservazione dei dati di traffico per esempio di accesso a internet per l’Italia è prevista di dodici mesi. Una risposta che arriva dopo dieci mesi è evidente che non consentirà molto probabilmente di andare a riconoscere la persona, perché, nel frattempo, si saranno in qualche modo bruciate le informazioni che sarebbero servite a fare il riconoscimento. Se c’è un intervento tecnico nell’immediato può essere proprio una attuazione rapida di queste modalità di accesso ai dati ».*

(193) Troppo spesso, attualmente, le piattaforme rispondono negativamente alle richieste dei pubblici ministeri, per esempio avanzando questioni legate alla *privacy* o non dando nemmeno risposta alla richiesta.

(194) La parola crittografia viene dal greco « *kryptos* », che significa nascosto, e si traduce letteralmente in « scrittura nascosta ». Può essere utilizzata per oscurare qualsiasi forma di comunicazione digitale, tra cui testo, immagini, video o audio. In pratica, la crittografia viene utilizzata principalmente per trasformare i messaggi in un formato illeggibile (noto come testo cifrato) che può essere decifrato in un formato leggibile (noto come testo in chiaro) solo dal destinatario autorizzato attraverso l’uso di una specifica chiave segreta.

(195) La crittografia nasce storicamente dalla necessità di assicurare la confidenzialità dei dati trasmessi, cioè la situazione in cui si vuole mantenere la segretezza di una comunicazione tra due o più utenti, in un contesto popolato anche da altre entità, potenzialmente malevole.

principali *social* con il Garante per la protezione dei dati personali, di registrare il codice *hash*<sup>(196)</sup> – la stringa alfanumerica che identifica un video o una immagine – così da evitare che qualcuno possa caricare il contenuto su un'altra piattaforma<sup>(197)</sup>.

La funzione di *hash* (o tecnica o sistema di *hashing*) è unidirezionale (*One Way Function*) e genera, a partire dal documento – sia esso di testo, immagine, video-immagine e/o audio, di qualsivoglia formato e dimensione –, una stringa alfanumerica la cui lunghezza (detta « *digest* » o « impronta » o, ancora, « valore di *hash* ») varia a seconda dell'algoritmo utilizzato ed è costante (non varia al variare della dimensione dei dati di *input*).

Le regole tecniche sulle firme elettroniche avanzate, qualificate e digitali – adottate con DPCM del 22 febbraio 2013, in attuazione del Codice dell'amministrazione digitale (decreto legislativo 7 marzo 2005, n. 82) – definiscono, all'articolo 1, la funzione di *hash* come « *una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti* ».

Come anticipato, l'algoritmo di *hash* è unidirezionale, nel senso che il suo valore non consente, partendo dall'impronta, di risalire direttamente al documento originario e si caratterizza per la forte resistenza alle collisioni, nel senso che è pressoché impossibile determinare due impronte uguali partendo da due differenti documenti.

Le caratteristiche del sistema di *hashing* sopradescritte ne hanno determinato il rilievo anche come tecnica di pseudonimizzazione particolarmente efficace nella protezione dei dati personali ai fini della rimozione del materiale illecito, dato che, una volta calcolata l'impronta (o *digest*), non è più necessaria la conservazione del *file* originale, contenente dati che possono portare a identificare, ad esempio, la vittima di *revenge porn*, utilizzato come « campione » di confronto per individuare tutti gli altri *file* nei cui confronti agire per impedirne la circolazione<sup>(198)</sup>.

(196) Gli *hash* sono il risultato di un algoritmo di *hashing* che mira essenzialmente a produrre una stringa unica e di lunghezza fissa, il valore *hash* o « *message digest* », per qualsiasi dato o « messaggio » dato.

(197) Nel 2017 Meta (all'epoca *Facebook*) ha creato un « progetto pilota » avviato inizialmente in Australia in collaborazione con l'Agenzia governativa per l'*E-Safety*, *The eSafety Commissioner*, e successivamente in altri Paesi fra i quali gli Stati Uniti, il Regno Unito, Canada e India, volto a bloccare, in via preventiva, la diffusione non consensuale di immagini e video a contenuto esplicitamente sessuale. Il programma consiste nella messa a disposizione della potenziale vittima di un canale sicuro di trasferimento per la trasmissione del materiale audiovisivo di cui teme la diffusione e che la piattaforma, una volta ricevuto, contrassegna con una tecnica di *hashing*; l'impronta viene conservata e il materiale cancellato entro il settimo giorno dal ricevimento. In Italia, dal 2020, tramite l'associazione no-profit « Permessonegato », il cui presidente, *Matteo Flora*, è stato audito il 10 novembre 2025, è stato reso possibile alle potenziali vittime partecipare a tale programma. Successivamente, a decorrere dall'8 marzo 2021 *Facebook* ne ha esteso l'accesso al Garante, sicché, a partire da tale data, chiunque – purché ultra quattordicenne – tema la pubblicazione sulla piattaforma di immagini e/o video intimi può dare impulso alla segnalazione accedendo alla pagina <https://www.garanteprivacy.it/temi/revengeporn>, scaricando l'apposito modello di segnalazione e inviandolo, una volta completato, all'indirizzo email ivi indicato.

(198) Tuttavia, è bene tenere a mente che la sicurezza di tale misura postula che il documento in chiaro, a cui applicare la funzione di *hash*, sia conservato separatamente dall'impronta, a soli fini probatori, e che entrambi siano oggetto delle opportune misure tecniche e organizzative in modo tale da ridurre il più possibile il rischio di re-

Se una donna ha fatto *sexting*, ossia ha condiviso un contenuto con il proprio compagno, e ha paura che quel contenuto possa essere diffuso senza il suo consenso su piattaforme o *social network*, può rivolgersi al Garante per la protezione dei dati personali che, in via preventiva, grazie a una collaborazione con META e altri *social* (non con tutte le piattaforme, purtroppo), può evitare che quel contenuto venga condiviso su altre piattaforme: registrando il codice *hash*, la piattaforma riconosce quel codice e se qualcuno tenta di caricarlo lo blocca.

Questo, a livello psicologico, aiuta tantissimo le potenziali vittime.

L'estensione alle altre piattaforme – a tutte quelle che invocano la crittografia come un diritto dei propri utenti – costituirebbe un grande passo avanti per la tutela delle vittime.

## 4.2 Gli ulteriori rimedi

Per Chiara Gius, coordinatrice nazionale del progetto Prin 2022 « rappresentazioni sociali della cyberviolenza contro donne e ragazze » e ricercatrice presso l'Università di Bologna<sup>(199)</sup>, occorre prevedere strumenti giuridici capaci di affrontare le difficoltà di identificare responsabilità multiple e diffuse, spesso distribuite su larga scala e rese anonime dalle architetture tecnologiche che, di fatto, rendono complesso, non solo il lavoro di identificazione della responsabilità, ma lo stesso procedimento istruttorio.

Per quanto riguarda il comparto tecnologico, è necessario un approccio che renda le aziende digitali responsabili per il ruolo che svolgono nel perpetuare o amplificare la violenza, data anche la loro capacità di trarre profitto da essa.

Il legislatore dovrebbero imporre obblighi di prevenzione *ex ante* e non solo di intervento *ex post*: urge una regolamentazione più stringente dei sistemi di *governance* algoritmica, della progettazione delle piattaforme e delle procedure di segnalazione e rimozione dei contenuti abusivi.

Le piattaforme devono garantire strumenti rapidi, trasparenti e accessibili per la tutela delle vittime, oltre che rendere espliciti i propri protocolli di intervento, solo così si può cominciare ad affrontare l'attuale percezione diffusa di impunità che caratterizza i reati informatici e che contribuisce alla sfiducia delle vittime nei confronti delle istituzioni e della giustizia.

Quanto mai opportuna – ha sottolineato Sandra Cioffi, presidente del Consiglio Nazionale degli Utenti<sup>(200)</sup> – è l'elaborazione di un testo unico dedicato alla violenza *on line* contro le donne, volto a ricomporre in modo organico norme, strumenti e responsabilità oggi distribuiti su più ambiti e fonti.

Della stessa opinione è Barbara Giovanna Bello, ricercatrice e docente di filosofia del diritto e di giustizia digitale presso l'Università

identificazione che è possibile avendo accesso ai dati di *input* e all'impronta. Sul punto si vedano i preziosi suggerimenti di S. CALOSSO, in <https://www.dataprotection-privacy.it/revange-porn-limpronta-di-hash-su-immagini-e-video-oggetto-di-segnalazione-ex-art-144-bis-codice-privacy/>.

(199) Audizione del 20 ottobre 2025.

(200) Audizione del 29 gennaio 2026.

degli Studi della Tuscia <sup>(201)</sup>, per la quale, non possiamo dire di essere sguarniti da disposizioni di prevenzione e contrasto della violenza di genere *on line*. Le norme, tuttavia, sono frammentate e la frammentazione rende la norma confusa e meno conoscibile. Si deve intervenire integrando le disposizioni lacunose e mettendole a sistema per assicurarne una maggiore efficacia.

Gli studi sull'efficacia delle disposizioni legislative dimostrano che l'entropia legislativa e la frammentazione delle norme rendono difficile la ricostruzione di un quadro unitario. In particolare, i principi di chiarezza e sintesi dei testi contribuiscono a far sì che le norme giuridiche possano essere conosciute non solo dalle potenziali vittime, ma anche dai potenziali autori.

---

(201) Audizione del 4 febbraio 2026.

Parte V  
LA POLIZIA POSTALE E DELLE COMUNICAZIONI

**1. La sicurezza informatica**

**1.1. Il dato normativo**

L'evoluzione tecnologica degli ultimi anni ha reso indispensabile l'uso di internet quale mezzo di scambio di informazioni, di accesso alle grandi banche dati, di esecuzione di transazioni e disposizioni finanziarie, di ideazione e creazione di nuove attività professionali.

La rapida diffusione di internet ha ben presto messo in evidenza i punti di debolezza della rete stessa, in particolar modo con riferimento alla sicurezza informatica.

È in questo scenario che nasce, con la riforma dell'amministrazione della Pubblica Sicurezza, la Polizia postale e delle comunicazioni, quale « specialità » della Polizia di Stato all'avanguardia nell'azione di prevenzione e contrasto della criminalità informatica e a garanzia dei valori costituzionali della segretezza della corrispondenza e della libertà di ogni forma di comunicazione.

Il principale sforzo operativo della Polizia postale è il continuo aggiornamento delle proprie conoscenze informatiche per fornire un'adeguata risposta alle sempre nuove frontiere tecnologiche della delinquenza.

Il decreto del Capo della Polizia – Direttore Generale della pubblica sicurezza del 28 giugno 2022 ha rideterminato l'assetto ordinativo, i compiti e le dotazioni organiche delle articolazioni periferiche della Polizia postale: la riorganizzazione ha delineando una nuova struttura organizzativa che ha a disposizione la rete dei 18 Centri Operativi per la Sicurezza Cibernetica (COSC) della Polizia postale, attivi nei principali capoluoghi di regione, e delle 82 Sezioni operative per la sicurezza cibernetica, presenti nelle province, al cui vertice è posto il rinnovato Servizio Polizia postale e per la sicurezza cibernetica, incardinato presso la Direzione centrale per la polizia scientifica e la sicurezza cibernetica del Dipartimento della pubblica sicurezza, dedicata all'alta investigazione tecnologica e alle scienze forensi.

Con decreto del Ministro dell'interno, di concerto con il Ministro dell'economia e delle finanze, firmato il 7 febbraio 2024, la nuova Direzione centrale per la polizia scientifica e la sicurezza cibernetica è diventata definitivamente operativa, assolvendo i compiti di coordinamento, direzione, pianificazione strategica e supporto centrale delle attività di polizia scientifica svolte dagli uffici della Polizia di Stato, nonché di coordinamento, direzione e pianificazione strategica dei servizi e delle attività svolte dalla Specialità della Polizia postale.

**1.2. I compiti**

*Ivano Gabrielli*, Dirigente superiore della Polizia di Stato e Direttore del Servizio Polizia postale e per la sicurezza cibernetica<sup>(202)</sup>, ha illustrato il funzionamento della Polizia postale e delle comunicazioni

(202) Audizione del 17 novembre 2025.

che è la struttura della Polizia di Stato deputata alla prevenzione e al contrasto al *cyber crime*.

Questa nuova tipologia di reati è il prodotto di un'evoluzione criminale che, in qualche modo, è cresciuta con la rete, con la sua diffusione e con la proiezione delle nostre vite e delle nostre economie nel dominio cibernetico.

L'Italia ha una forza di polizia dedicata al *cyber crime* tra le più risalenti.

Il *cyber crime* è sussumibile in tre grandi famiglie.

Ci sono i reati contro il patrimonio: frodi *on line*, attacchi ai sistemi economici finanziari, falso *trading on line*, false offerte d'investimento, tutto ciò che si muove attorno ai *crypto asset* anche in tema di proiezione di attività di criminalità organizzata. Oggi tutti noi abbiamo servizi di *internet banking*, gestiamo le nostre risorse attraverso l'*home banking*, le disposizioni economiche finanziarie si sono virtualizzate, gli stessi istituti bancari non vengono più presidiati fisicamente, ma virtualmente. I più grandi investimenti in termini di sicurezza oggi vengono fatti nel dominio cibernetico anche per questo settore.

La seconda famiglia è rappresentata dai reati nativi informatici, i cosiddetti *cyber attack*: accessi abusivi e danneggiamento ai sistemi informatici. Il riferimento è a tutti quei reati che, in qualche modo, ledono e violano un perimetro informatico per portare fuori dati.

Infine, ci sono i reati contro la persona commessi attraverso la rete. Si tratta dei primi reati di cui la Polizia postale si è occupata fin dal 1998 con precipuo riferimento allo sfruttamento sessuale dei minori *on line*. La pedopornografia è il primo reato cibernetico che tutte le polizie del mondo si sono trovate ad affrontare. Gli altri reati sono il frutto della proiezione in rete di quelli tradizionali: minacce, molestie e *stalking*, che ha una dimensione cibernetica molto importante.

I reati contro la persona, ancorché caratterizzati dal genere, hanno una forte componente cibernetica. Spesso sono «reati sentinella». È capitato che alcuni fatti di sangue venissero anticipati da comportamenti attuati a livello digitale sotto forma di pedinamento elettronico, di accesso abusivo ai profili della vittima, integranti veri e propri atti persecutori. Tra i reati digitali accertati dalla Polizia postale si segnala il *revenge porn*, cioè la diffusione di materiale intimo senza il consenso del soggetto ritratto, il *sextortion*, l'estorsione sessuale quale conseguenza dell'acquisizione di immagini intime, fino ad arrivare all'illecita diffusione di immagini generate da sistemi di intelligenza artificiale.

Negli ultimi anni, in Italia e a livello internazionale, si è registrato un incremento delle violenze di genere digitali sotto forma di diffusione non consensuale di immagini intime, di campagne di odio sui *social*, di creazione di siti e *community* che normalizzano o incentivano comportamenti sessisti e misogini, fino ad arrivare allo *stalking* e alle molestie *on line*.

Sono condotte che colpiscono la dignità, compromettono la libertà di espressione e di autodeterminazione, provocando danni psicologici profondi. La diffusione di contenuti sessisti e discriminatori sul *web*, attraverso le piattaforme digitali, rappresenta una delle forme più insidiose di violenza contemporanea. La rete internet, nata come spazio di libertà e condivisione, viene spesso utilizzata per alimentare odio, denigrazione e sfruttamento, in particolare ai danni delle donne. I

*social media* e le piattaforme di condivisione, grazie all'interconnessione globale tra le reti informatiche e di telecomunicazioni, hanno la capacità di rendere rapidamente virali i contenuti amplificando l'impatto della violenza.

Questo è il connotato fondamentale della dimensione digitale dei reati: il fatto di poter permanere in rete, creando una vittimizzazione di secondo livello.

A questo si è aggiunto, di recente, l'utilizzo dell'intelligenza artificiale: *deepfake*, foto, video e audio creati grazie a *software* che, partendo da contenuti reali, modificano o creano caratteristiche, movimenti di un volto, di un corpo e la voce di una persona. Proliferano i *deepfake*, i *deepnude* che riguardano spesso persone ignare di essere rappresentate nude o in contesti pornografici. Con la tecnologia del *deepnude*, i visi delle persone – compresi i minori, purtroppo – possono essere innestati, di fatto, su corpi di altre e possono essere denudati ricostruendo l'aspetto che avrebbe il corpo sotto gli indumenti e creando immagini altamente realistiche.

L'attività di prevenzione della Polizia postale viene svolta su più livelli, attraverso l'informazione.

L'Unità di analisi del crimine informatico <sup>(203)</sup> è costituita da un gruppo di esperti, da una équipe di psicologi della Polizia di Stato che ogni anno – oltre a dare un supporto nell'attività di *profiling* e di investigazione, soprattutto nelle indagini particolarmente complesse, quali quelle che riguardano la sfera dei minori – costruiscono contenuti da erogare in una serie di incontri con moduli che vengono proposti per contenuti diversi in base alla età avvalendosi di campagne di informazione quale, ad esempio, la campagna « *Una vita da social* », sostenuta dal Ministero dell'istruzione, una campagna itinerante della Polizia postale <sup>(204)</sup>.

(203) L'unità di analisi sul crimine informatico (*Computer Crime Analysis Unit*) è composta da personale tecnico e investigativo. La sua funzione è di affiancare gli investigatori della Polizia postale e delle comunicazioni nelle indagini sui crimini ad alta tecnologia, progettando nuove tecniche investigative e tracciando profili psicologici e comportamentali degli autori di tali crimini. Le principali attività della struttura sono: ricerche e studi sul fenomeno della criminalità informatica in collaborazione con università, aziende e istituzioni; sperimentazione di nuove tecniche investigative in materia di *computer crime*; progettazione di percorsi di formazione sulla sicurezza informatica e *computer crime* in collaborazione con università e aziende; divulgazione di informazioni e risultati di ricerche in contesti scientifici; assistenza psicologica degli investigatori che si occupano di *computer crime* (pedofilia).

(204) La Polizia di Stato con il progetto « *Una vita da social* », si rivolge a studenti, insegnanti e familiari, per metterli in guardia dai pericoli della rete e diffondere un corretto e consapevole uso dei *social network*. La campagna di educazione alla legalità su internet ha carattere itinerante su tutto il territorio nazionale. All'interno di un autocarro (*truck*) gli specialisti della Polizia postale illustrano ai visitatori le principali insidie della rete, fornendo consigli per una navigazione sicura. Il percorso del *truck* è stato riassunto su una mappa, sulla quale sono evidenziate tutte le tappe. Passando con il *mouse* sulle città si apre un *box* con i principali eventi che hanno caratterizzato ogni singola tappa. Dalla sua nascita, « *Una Vita da Social* » ha raggiunto 4 milioni e mezzo di studentesse e studenti, toccando più di 700 città italiane e anche alcune città all'estero. Le pagine *social* ufficiali su *X* e *Facebook*, ulteriore strumento di diffusione della cultura della sicurezza *on line*, contano oggi oltre 130mila *follower*. « *Una Vita da Social* » segue le esigenze delle nuove generazioni e i temi che più stanno loro a cuore per offrire loro strumenti concreti per affrontare il *web* in modo sicuro, responsabile e consapevole, anche nel rispetto delle Linee guida del Ministero dell'istruzione e del merito per l'insegnamento dell'educazione civica e relative alla cittadinanza digitale.

Promossa dalla Polizia di Stato e dal Ministero dell'istruzione e del merito, nell'ambito del progetto «*Generazioni Connesse*», l'iniziativa mira a sensibilizzare studentesse e studenti, ma anche docenti e famiglie, all'uso responsabile di internet e dei *social*, affrontando tematiche cruciali come il cyberbullismo, l'adescamento *on line* e l'educazione sentimentale in rete. I messaggi chiave dell'ultima edizione richiamano l'importanza di mantenere sempre un'attenzione consapevole ai propri comportamenti, sia *on line* che *off line*, e l'invito a non restare indifferenti di fronte alle compagne e ai compagni in difficoltà e a promuovere il rispetto, l'ascolto e l'utilizzo della rete come strumento di inclusione e condivisione. Il progetto, già da alcune edizioni, si è arricchito di contenuti dedicati all'educazione stradale e alla lotta contro ogni forma di discriminazione, ampliando così il proprio messaggio formativo.



*Una delle tappe del truck della Polizia postale nell'ambito del progetto « Una vita da Social ».*

Il gruppo di lavoro prevede e intercetta i fenomeni più comuni, dalle sfide, c.d. « *challenge* »<sup>(205)</sup>, alla cosiddetta « *body positivity* »<sup>(206)</sup>.

Quest'anno – ha proseguito *Ivano Gabrielli* nel corso della sua audizione – abbiamo proiettato nelle scuole «... *un filmato, un cortometraggio dedicato alla body positivity, quindi alla relazione tra le persone giovani rispetto al modello di bellezza che viene proposto, che spesso è foriero di una serie di problemi che sfociano – anche qui – in atti di violenza. Altre campagne sono state dedicate alle relazioni tra ragazzi che utilizzano i social, anche qui sfruttando le potenzialità di produzioni artistiche prodotte in collaborazione con la RAI (il cortometraggio 101%), che accompagnano un percorso non di educazione, ma di vera e propria informazione, che deve aiutare le persone, soprattutto i più giovani, a costruirsi in una dimensione sociale estremamente diversa* ».

La Polizia postale lavora con le nuove generazioni, con i cittadini di domani, mettendo a disposizione: strumenti di sicurezza; strumenti tecnologici; la capacità di mettere in sicurezza un *device* dato ad un minore; strumenti di *alerting*, di conoscenza che permettono di riconoscere un profilo *fake* che in quel momento mi sta contattando.

L'intento è quello di introdurre un principio di rispetto nei rapporti umani che deve essere declinato in maniera diversa quando parliamo di rapporti tecno-mediati, oggi così integrati, così presenti nella sfera delle nostre relazioni sociali.

(205) Le *challenge* sono sfide o attività alle quali soprattutto i più giovani partecipano su internet, spesso per dimostrare coraggio o resistenza fisica. Molto diffuse sui *social media*, possono variare da attività creative a situazioni pericolose.

(206) Il *body positivity* è il movimento per l'accettazione di ogni corpo e si inserisce nella lotta al *body shaming*.

Parte VI  
LA PROTEZIONE OFFERTA DALLE *AUTHORITY*

**1. L'Autorità per le garanzie nelle comunicazioni (AGCOM)**

**1.1 La natura e le funzioni**

L'Autorità per le garanzie nelle comunicazioni è un'autorità indipendente, istituita dalla legge 31 luglio 1997, n. 249.

Indipendenza e autonomia sono elementi costitutivi che ne caratterizzano l'attività e le deliberazioni.

L'AGCOM è innanzitutto un'autorità di garanzia: la legge istitutiva affida all'Autorità il duplice compito di assicurare la corretta competizione degli operatori sul mercato e di tutelare i consumi di libertà fondamentali degli utenti.

L'Autorità per le garanzie nelle comunicazioni è un'autorità « convergente » e, in quanto tale, svolge funzioni di regolamentazione e vigilanza nei settori delle comunicazioni elettroniche, dell'audiovisivo, dell'editoria, delle poste e più recentemente delle piattaforme *on line*.

I profondi cambiamenti determinati dalla digitalizzazione del segnale, che ha uniformato i sistemi di trasmissione dell'audio (inclusa la voce), dei video (inclusa la televisione) e dei dati (incluso l'accesso a internet), sono alla base della scelta del modello convergente, adottato dal legislatore italiano e condiviso da altre autorità di settore a livello europeo e internazionale <sup>(207)</sup>.

**1.2 I poteri sulle piattaforme**

L'AGCOM, come riferito dal presidente *Giacomo Lasorella* <sup>(208)</sup>, a partire dal 2023, ha assunto anche il ruolo di coordinatore dei servizi digitali per l'Italia, il c.d. *digital service coordinator*, ai sensi del *Digital Services Act* (DSA, Regolamento 2022/2065/UE) che è la normativa quadro di riferimento in questa materia.

Il principio di fondo – introdotto dalla c.d. Direttiva *e-commerce* (Direttiva 2000/31/CE) che riproduce l'analogo principio stabilito nella cosiddetta Sezione 230 del *Communications Decency Act* degli Stati Uniti del 1997 – è che le piattaforme non sono responsabili per i contenuti immessi dagli utenti.

Il DSA ha confermato questa regola cardine prevedendo, tuttavia, una serie di obblighi di trasparenza a carico delle piattaforme.

Tale impostazione presenta, tuttavia, evidenti profili critici nei casi in cui l'illegalità assuma carattere sistematico, stabile e largamente riconoscibile. In presenza di comunità *on line* di dimensioni molto rilevanti, concentrate in uno specifico contesto nazionale e coinvolte per lungo tempo in condotte penalmente illecite, l'automatica esclusione di responsabilità della piattaforma appare difficilmente sostenibile. Si impone, pertanto, una revisione del regime di responsabilità nei

(207) Al pari delle altre autorità previste dall'ordinamento italiano, l'AGCOM risponde del proprio operato al Parlamento, che ne ha stabilito i poteri, definito lo statuto ed eletto i componenti.

(208) Audizione del 23 ottobre 2025.

casi di consapevole inerzia, tolleranza protratta o mancata adozione di misure adeguate a fronte di fenomeni illeciti manifesti e persistenti.

Per le piattaforme molto grandi<sup>(209)</sup>, poi, sono stati previsti ulteriori obblighi a tutela dei minori e un meccanismo che le obbliga ad analizzare i cosiddetti « rischi sistemici » (*l'assessment*) connessi all'attività e a predisporre delle misure di mitigazione.

La Commissione europea – competente per le piattaforme molto grandi (*very large online platforms and search engines*) come META, Google o Booking – opera una valutazione di queste misure attraverso un'attività sostanzialmente di controllo, a seguito della quale può eventualmente irrogare delle sanzioni.

Per la determinazione della competenza dei singoli Stati, opera il principio del Paese di origine che governa la quasi totalità del quadro dell'attività europea e radica la competenza dell'autorità del Paese nel quale il soggetto risiede: il Paese che subisce la violazione segnala all'autorità nazionale del Paese di origine la questione.

Tale modello presenta, peraltro, evidenti criticità applicative, poiché non appare sempre garantita l'effettiva capacità della Commissione europea e delle autorità dello Stato di stabilimento di intervenire con adeguata tempestività e conoscenza del contesto nazionale nei casi di diffusione di contenuti illeciti o dannosi. Il problema si accentua ove tali contenuti siano rivolti a uno specifico pubblico nazionale, pur essendo diffusi da piattaforme stabilite in altri Stati membri, nonché in ragione della concentrazione di molte grandi piattaforme in un numero limitato di Paesi, con conseguente rischio di sovraccarico delle relative autorità di controllo.

Il presidente dell'AGCOM Giacomo Lasorella ha osservato che « Il Digital Services Act è essenzialmente un regolamento procedurale: non stabilisce divieti o obblighi che sono rimessi alle determinazioni delle legislazioni nazionali ». In particolare, l'AGCOM non ha il potere di ordinare la chiusura di siti, ma ha, per esempio, il potere di ordinare la rimozione di contenuti illeciti. La competenza è delle autorità nazionali alle quali, i singoli Stati, attribuiscono poteri specifici.

Le *very large online e video sharing platforms*, che consentono agli utenti di immettere direttamente contenuti video – come Youtube – sono regolate dalla c.d. Direttiva SMAV, sui servizi di *media* audiovisivi (Direttiva 2018/1808/UE del 14 novembre 2018).

La Direttiva SMAV, che regola in generale il settore dell'audiovisivo, disciplina anche i contenuti delle *very large online platforms* attribuendo alle autorità il potere di bloccare i contenuti illeciti e dannosi per i minori e più in generale per la dignità umana.

In applicazione del principio del Paese di origine, l'AGCOM ha predisposto un regolamento con due modalità di intervento.

La prima è una procedura urgente che consente di inibire immediatamente determinati contenuti illeciti (entro tre giorni). Sono tali i programmi, i video e le comunicazioni commerciali generati dagli utenti che incitano all'odio razziale, sessuale, religioso, etnico e che violano la dignità umana. In questi casi, pur applicandosi il principio

(209) Piattaforme con un numero medio mensile di destinatari attivi del servizio nell'Unione europea pari o superiore a 45 milioni.

del Paese di origine, l'autorità di destinazione può limitare la libera circolazione di questi contenuti se diretti al pubblico italiano.

Per l'avvio della procedura occorre la segnalazione dell'utente. Nel caso in cui ricorra una situazione di urgenza, ossia il rischio di un pregiudizio grave, imminente e irreparabile, l'autorità può avviare, entro cinque giorni, un procedimento nei confronti della *video sharing platform* che, se non si adegua nei successivi cinque giorni rimuovendo il contenuto, diventa destinataria di un ordine al quale la piattaforma deve ottemperare entro tre giorni, salvo che non impugni il provvedimento.

In tutti gli altri casi, quelli non urgenti, l'autorità dispone la trasmissione degli atti all'autorità nazionale competente dello Stato membro.

Merita evidenziare che il procedimento delineato dal regolamento AGCOM, pur contemplando l'attivazione anche d'ufficio, presenta una scansione temporale che rischia di ridurne l'effettiva tempestività rispetto alla rapidità di diffusione dei contenuti illeciti o dannosi online. In tale quadro, la rilevanza assunta in concreto dalle segnalazioni degli utenti appare suscettibile di limitare l'efficacia complessiva del sistema, rendendo opportuno un rafforzamento dei poteri e degli strumenti di monitoraggio proattivo da parte dell'Autorità in un mondo vasto come quello del *web*. L'esperienza applicativa richiamata dalla stessa AGCOM conferma, del resto, l'esigenza di presidi regolatori più incisivi ed effettivi.

### 1.3 Il gruppo Facebook « Mia moglie »

Nel gruppo pubblico, creato nel 2019 sulla piattaforma *on line Facebook*, denominato « Mia moglie », al quale risultavano iscritti oltre 32.000 utenti, principalmente uomini, venivano pubblicate e soprattutto commentate immagini o video sessualmente espliciti non soltanto delle partner dei componenti del gruppo ma anche di colleghe e persino di sconosciute scattate segretamente od ottenute illecitamente<sup>(210)</sup>. Il gruppo è stato immediatamente chiuso da META per violazione delle *policy* e per la pressione mediatica che ne è conseguita.

L'AGCOM, dal canto suo, ha chiesto a META delle informazioni per poter segnalare la questione alla Commissione europea che, come detto, è competente per le piattaforme molto grandi.

Tale vicenda costituisce un significativo banco di prova circa la necessità di affinare gli attuali strumenti di tutela della dignità e dell'incolumità delle donne, e più in generale delle persone, nell'ecosistema digitale. Appare infatti particolarmente rilevante che un gruppo di oltre 32.000 utenti, localizzato in Italia, abbia potuto per lungo tempo veicolare contenuti suscettibili di rilievo penale senza tempestiva

(210) Come evidenziato da Lucia Bainotti, Assistant Professor in Digital and Visual Media Analysis presso il Dipartimento di Media Studies dell'Università di Amsterdam (audita il 17 novembre 2025), i contenuti condivisi, come nel caso del gruppo Facebook « Mia Moglie », non sono necessariamente sessualmente espliciti. Spesso si tratta di foto di telecamere nascoste, per esempio, nei camerini oppure telecamere nascoste in contesti come la spiaggia oppure riprese fatte di nascosto nei supermercati. Quindi, pur non essendo immagini sessualmente esplicite, si tratta di immagini intime che vengono condivise senza il consenso e che vengono anche accompagnate da termini misogini, commenti denigratori e forme di linguaggio d'odio a tutti gli effetti.

emersione del fenomeno né effettiva assunzione di responsabilità da parte della piattaforma ospitante. Una simile condizione di sostanziale evanescenza della responsabilità difficilmente troverebbe riscontro nell'ordinamento interno, nel quale, anche alla luce dei principi generali del diritto civile, emergerebbero profili di corresponsabilità del soggetto che mette a disposizione e organizza l'infrastruttura. Resta pertanto evidente l'esigenza di rafforzare i presidi che impongano interventi effettivi e tempestivi, senza attendere che la conoscenza dell'illecito divenga ineludibile per effetto della sua pubblica emersione.

Come raccontato da *Laura Bononcini*, *Public Policy Director* di Meta per il Sud-Europa <sup>(211)</sup>, il gruppo è stato creato nel 2019 ed è rimasto inattivo fino ad aprile-maggio del 2025. Dopodiché, sono iniziate le attività che poi hanno portato, il 20 agosto 2025, alla rimozione per violazione della *policy* in materia di sfruttamento sessuale degli adulti. Man mano che arrivavano le segnalazioni da parte degli utenti, ma anche, in alcuni casi, sulla base di identificazioni, grazie all'intelligenza artificiale, di contenuti che violavano le *policy*, questi singoli contenuti sono stati rimossi dal gruppo e in alcuni casi sono state anche prese iniziative nei confronti degli utenti che caricavano i contenuti <sup>(212)</sup>.

La «*red line*» di Meta per la rimozione di un gruppo o di una pagina viene raggiunta quando si verificano ripetute violazioni degli *standard* della *community* monitorate tramite un sistema di *strike*. Ci sono diversi livelli di *strike*: quelli più gravi possono determinare la rimozione immediata del gruppo, quelli meno gravi, invece, dei singoli contenuti.

La decisione di rimuovere l'intero gruppo è stata il risultato di una revisione dettagliata che ha fatto emergere violazioni in particolare nella parte destinata ai commenti alle immagini e ai contenuti condivisi.

Di estremo interesse, al riguardo, è l'osservazione di *Lilia Giugni*, professoressa di Innovazione inclusiva presso l'*University College* di Londra e ricercatrice di Innovazione sociale presso l'Università di Cambridge <sup>(213)</sup>, secondo cui le piattaforme *social* di massa, i *social mainstream*, sulla carta bandiscono le immagini esplicite non consensuali, nonché molti altri contenuti violenti o misogini, come il discorso d'odio. Nella pratica, però, come dimostrato dai tanti casi di cronaca recenti, tra cui quello italiano del gruppo *Facebook* «*Mia Moglie*», non solo ospitano, ma facilitano svariate forme di abuso.

Esiste un legame molto stretto tra violenza digitale di genere e strategie economiche di *data mining*, cioè le strategie di raccolta e monetizzazione dei dati personali, tipiche dei grandi *social media*.

Per tenere gli utenti il più possibile incollati alla tastiera, la maggior parte delle piattaforme *social* favorisce sistematicamente e algoritmicamente la circolazione di contenuti divisivi, capaci cioè di suscitare emozioni forti, come la rabbia e quindi di stimolare ulteriori interazioni.

(211) Audizione del 27 novembre 2025.

(212) A seconda della gravità si può anche arrivare alla rimozione dell'*account* da cui vengono postati questi contenuti.

(213) Audizione del 17 novembre 2025.

Inoltre, grazie al proprio *design* algoritmico, le piattaforme manipolano i materiali visualizzati da ogni utente, anche e soprattutto in funzione dei contenuti che quell'utente ha già visualizzato in precedenza: una volta che una persona ha, ad esempio, iniziato a consumare o a postare su una piattaforma dei contenuti sessisti, se ne vedrà proporre di simili dall'algoritmo della piattaforma stessa.

La combinazione di questi due meccanismi è proprio alla base della rapida e massiccia viralizzazione di molte forme di abuso *on line* ed è anche una delle principali cause della radicalizzazione di tanti utenti in gruppi *social* misogini, quali appunto « Mia Moglie ».

I meccanismi descritti evidenziano la necessità di prevedere sotto il profilo normativo la corresponsabilità delle piattaforme nel veicolare contenuti dannosi o illeciti che assumono proporzioni significative sul *web*.

#### 1.4 La piattaforma « *Phica.eu* »

Sul sito *web Phica.eu* si trovava un *forum on line* di origine italiana, creato nel 2005, a cui erano iscritti 700.000 utenti e in cui venivano pubblicate e scambiate fotografie all'insaputa delle donne ritratte.

Anche in questo caso, le immagini, spesso modificate, venivano accompagnate da commenti sessisti, volgari e violenti. Tra le donne coinvolte vi erano non solo figure pubbliche e politiche, ma anche donne prive di ruoli pubblici o di notorietà. La pressione che ne è seguita, anche in questo caso, ha determinato il gestore alla chiusura del sito che, comunque, è posto sotto sequestro da parte della magistratura italiana che ha avviato una vasta indagine.

*Silvia Semenzin*<sup>(214)</sup> ha rivelato che su questa piattaforma c'erano sezioni, come la sezione *spy*, in cui gli uomini si educavano a vicenda su come nascondere le videocamere nelle palestre, nei camerini dei negozi, nelle scuole, nelle università. C'erano uomini che si offrivano volontari per spogliare le donne con la tecnologia, uomini che offrivano foto e video delle proprie mogli alla mercé degli sguardi altrui, uomini che chiedevano come usare gli *spyware* per controllare le proprie fidanzate. Nonostante la pagina oggi sia stata chiusa, il problema rimane, perché non basta chiudere una piattaforma per poter far fronte a questo tipo di fenomeno così pervasivo.

Il problema rimane, questi utenti migrano da una piattaforma all'altra con la sensazione di rimanere impuniti, spostandosi dove sono meno monitorati. È il caso di *Telegram*. Ora i canali si sono moltiplicati. Ci sono poi tantissime altre piattaforme, come « *Reddit* » o piattaforme minori pornografiche, anche a livello internazionale, dove gli utenti italiani continuano a riprodurre queste dinamiche.

Le modalità di intervento sul sito *Phica.eu* sono state illustrate in dettaglio da *Giacomo Lasorella*, presidente dell'Autorità per le garanzie nelle comunicazioni<sup>(215)</sup>: l'AGCOM si è interfacciata con la Polizia postale e ha accertato che il sito era riferibile a una persona fisica, tale *Vittorio Vitiello*, che ha affittato uno spazio *cloud* gestito da un *hosting provider* francese, *OVH*, provvedendo a personalizzarne l'architettura.

(214) Audizione del 16 ottobre 2025.

(215) Audizione del 23 ottobre 2025.

I nomi a dominio dei siti internet risultano registrati a nome di *GoDaddy.com LLC*, una società di diritto inglese, per conto di un gestore che non è stato possibile identificare. La società *Cloud seeding corporations*, con base negli Stati Uniti, ha un rappresentante in Belgio che opera come fornitore di servizi intermediari. I servizi di *hosting* risultano forniti dalla società *OVH SAS* stabilita in Francia. Lo stesso soggetto ha costruito una società, tale *Lupotto S.r.l.*, con l'obiettivo di gestire i *banner* pubblicitari all'interno della piattaforma. Questo quadro, alla luce delle competenze delineate all'inizio, rende particolarmente tortuoso individuare e sanzionare i soggetti coinvolti.

L'AGCOM, relazionandosi con l'omologo francese ARCOM (*Autorité de régulation de la communication audiovisuelle et numérique*), ha attivato i meccanismi di cooperazione, ma tecnicamente, proprio perché il sito è riferibile a una società che ha sede in Francia, la competenza è dell'autorità francese alla quale l'Italia non ha potuto far altro che trasmettere la segnalazione.

La Commissione europea, una volta raccolte le segnalazioni, può contestare le violazioni ai responsabili e comminare sanzioni, la cui entità può arrivare sino al 6% del fatturato europeo.

L'individuazione del responsabile è avvenuta ad opera di *Alex Orlowski*, esperto di *cyberintelligence* che è riuscito a risalire al responsabile del sito, condividendo le proprie ricerche con la Polizia postale, a conferma della necessità di una stretta collaborazione pubblico-privato in questo campo.

Sentito da questa Commissione di inchiesta<sup>(216)</sup>, ha raccontato di far parte di un piccolissimo *team* con sede a Parma e anche a Barcellona spiegando di aver utilizzato le tecniche « *che utilizzano gli stessi hacker, nel senso che abbiamo utilizzato tecniche di analisi della pagina, quindi andando in profondità nei server, dove erano i server eccetera, ma, cosa molto importante, tutti lasciano delle tracce on line: io dico sempre che non esiste l'anonimato on line, è veramente difficile mantenerlo, perché tutti lasciamo delle tracce. Il gestore del sito utilizzava sempre degli avatar di gatti. Da questi avatar di gatti, facendo delle ricerche su quelli che sono i leak nel dark web, abbiamo cercato ad esempio nomi simili al sito in questione, per vedere se in tutti questi dati ... ci fosse qualcosa. Veramente tutto è nato da X, dove abbiamo trovato un vecchissimo account di Twitter che diceva che la pagina era giù per un problema di server francesi. Quindi, noi siamo andati a cercare tutti i leak dei server francesi, se c'era qualcuno che aveva utilizzato come nick o come password il nome del sito in questione. Lì abbiamo trovato i primi dati, quindi abbiamo scoperto che i server fino al 2018, penso, erano in Francia. Poi abbiamo analizzato tutti quelli che erano i redirect e i clickbait: quando si andava sulla pagina si aprivano tantissime altre pagine di pubblicità, quindi da questi codici abbiamo scoperto tutta quella che era la rete dove monetizzava grazie a questi contenuti. Abbiamo dunque utilizzato il dark web, come farebbero i criminali, per trovare il nome, la e-mail e anche il cellulare della persona incriminata. È quello che si chiama un lavoro di OSINT, che vuol dire "open-source intelligence". Ovviamente per fare questo bisogna anche accedere al dark* »

(216) Audizione del 10 novembre 2025.

web, che non è uno dei posti migliori dove andare; è come andare in un bar di delinquenti, in un porto di una nazione molto lontana ».

La vicenda esaminata evidenzia come l'attività di individuazione e contrasto delle condotte illecite non possa gravare esclusivamente sulle Autorità pubbliche, chiamate a intervenire *ex post* con strumenti spesso resi meno efficaci dalla frammentazione transnazionale delle responsabilità. Essa conferma, infatti, la necessità che le piattaforme e i prestatori di servizi digitali, in quanto soggetti che dispongono ovvero sono nella condizione di disporre di adeguati strumenti tecnici, organizzativi e informativi, assumano un ruolo attivo nella prevenzione del misuse delle proprie funzioni e dei propri servizi, adottando misure idonee a impedire, rilevare tempestivamente e segnalare condotte illecite.

### 1.5 Le criticità e i rimedi

Venendo allo scandalo dei *social* di Meta e dei gruppi sessisti e dei siti con contenuti pornografici – ha proseguito Giacomo Lasorella, presidente dell'Autorità per le garanzie nelle comunicazioni <sup>(217)</sup> – il *Digital Services Act* (Regolamento 2022/2065/UE) interviene soprattutto sulle relazioni massive, non offrendo piena tutela in presenza di violazioni che riguardano i singoli.

Ad ogni modo già il DSA, all'articolo 34, lettera d), prevede che le piattaforme di grandi dimensioni debbano effettuare ogni anno valutazioni di rischio per evitare anche la violenza di genere <sup>(218)</sup>.

L'articolo 18 del *Digital Services Act* prevede, inoltre, che quando un *social* viene a conoscenza di informazioni che fanno sospettare che siano commessi reati deve collaborare con gli Stati membri fornendo tutte le informazioni necessarie.

Uno strumento utile, da implementare, è quello dei reclami all'AGCOM, previsto dall'articolo 53 del DSA. La norma, rubricata « *Diritto di presentare un reclamo* », prevede che i destinatari del servizio, nonché gli organismi, le organizzazioni o le associazioni incaricati di esercitare per loro conto i diritti conferiti dallo stesso DSA, hanno il diritto di presentare un reclamo nei confronti dei fornitori di servizi intermediari vertente sulla violazione del DSA presso il coor-

(217) Audizione del 23 ottobre 2025.

(218) Articolo 34 (Valutazione del rischio), « 1. I fornitori delle piattaforme on line di dimensioni molto grandi e di motori di ricerca on line 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 ».

dinatore dei servizi digitali dello Stato membro in cui il destinatario del servizio è situato o è stabilito. Il coordinatore dei servizi digitali valuta il reclamo e, se del caso, lo trasmette al coordinatore dei servizi digitali del luogo di stabilimento, accompagnato, ove ritenuto appropriato, da un parere. Se il reclamo rientra fra le responsabilità di un'altra autorità competente nel suo Stato membro, il coordinatore dei servizi digitali che riceve il reclamo lo trasmette a tale autorità. Nel corso del procedimento, entrambe le parti hanno il diritto di essere ascoltate e di ricevere informazioni adeguate sullo stato del reclamo, conformemente al diritto nazionale.

Si osserva, tuttavia, che la procedura descritta presenta un evidente profilo di debolezza, in quanto la sua eccessiva articolazione e complessità regolatoria e sanzionatoria rischia di comprometterne l'effettività, non risultando pienamente idonea ad assicurare l'adozione di misure tempestive, afflittive e realmente dissuasive nei confronti dei soggetti che violano il quadro normativo. In tale prospettiva, appare pertanto necessario riconoscere alle autorità nazionali, con particolare riguardo ai casi che producono effetti circoscritti al singolo Stato membro, poteri di intervento più ampi e più celeri, così da garantire una risposta più immediata ed efficace alle violazioni accertate.

Infine, mentre per le televisioni tradizionalmente c'è una responsabilità editoriale, che l'AGCOM ha fatto più volte valere in occasione di ordini specifici di eliminazione di determinati contenuti, per il *web* permangono le difficoltà di intervento illustrate.

Sicuramente avere più poteri, come per esempio quello di bloccare determinati siti, consentirebbe un intervento più efficace, e su questo tema — ha concluso il dottor *Giacomo Lasorella* — «*ci siamo, siamo pronti a continuare questa interlocuzione e ovviamente a trovare anche i modi, con le altre autorità "consorelle" europee, per una tutela quanto più possibile efficace*».

## **2. Il Garante per la protezione dei dati personali**

### **2.1 La natura e le funzioni**

Il Garante per la protezione dei dati personali è l'autorità amministrativa indipendente incaricata di tutelare i diritti e le libertà fondamentali, garantendo il rispetto della dignità nelle operazioni di trattamento dei dati personali.

Istituito nel 1996, con la cosiddetta legge sulla *privacy* (legge 31 dicembre 1996, n. 675) e successivamente disciplinato dal Codice in materia di protezione dei dati personali (decreto legislativo n. 196 del 2003), il Garante ha il compito principale di garantire che il trattamento dei dati personali sia conforme alla legislazione nazionale e al Regolamento 2016/679/UE (GDPR). Il codice della *privacy* è stato aggiornato alla luce delle novità introdotte dal GDPR tramite il decreto legislativo 10 agosto 2018, n. 101, per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679.

Il Garante collabora attivamente con le altre autorità di controllo europee, offrendo supporto reciproco per garantire una corretta e uniforme applicazione del Regolamento.

Inoltre, il Garante per la protezione dei dati personali:

- controlla che i trattamenti di dati personali siano conformi al Regolamento nonché a leggi e regolamenti nazionali e prescrive, ove necessario, ai titolari o ai responsabili dei trattamenti le misure da adottare per svolgere correttamente il trattamento nel rispetto dei diritti e delle libertà fondamentali degli individui;
- collabora con le altre autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del Regolamento;
- esamina i reclami;
- rivolge, nel caso di trattamenti che violano le disposizioni del Regolamento, ammonimenti al titolare e del trattamento o al responsabile del trattamento e ingiunge di conformare i trattamenti alle disposizioni del Regolamento, impone una limitazione provvisoria o definitiva del trattamento, incluso il divieto di trattamento o ordina la rettifica, la cancellazione di dati personali o la limitazione del trattamento;
- adotta i provvedimenti previsti dalla normativa in materia di protezione dei dati personali;
- segnala, anche di propria iniziativa, al Parlamento e altri organismi e istituzioni l'esigenza di adottare atti normativi e amministrativi relativi alle questioni riguardanti la protezione dei dati personali;
- formula pareri su proposte di atti normativi e amministrativi;
- partecipa alla discussione su iniziative normative con audizioni presso il Parlamento;
- predispone una relazione annuale sull'attività svolta e sullo stato di attuazione della normativa sulla *privacy* da trasmettere al Parlamento e al Governo;
- partecipa alle attività dell'Unione europea e internazionali di settore, anche in funzione di controllo e assistenza relativamente ai sistemi di informazione Europol, Schengen, VIS (*Visa Information System*), e altri;
- cura l'informazione e sviluppa la consapevolezza del pubblico e dei titolari del trattamento in materia di protezione dei dati personali, con particolare attenzione alla tutela dei minori;
- tiene registri interni delle violazioni più rilevanti e impone sanzioni pecuniarie ove previsto dal Regolamento e dalla normativa nazionale;
- coinvolge, ove previsto, i cittadini e tutti i soggetti interessati con consultazioni pubbliche dei cui risultati si tiene conto per la predisposizione di provvedimenti a carattere generale.

## 2.2 Il reclamo al Garante

L'articolo 141 del decreto legislativo n. 196 del 2003 prevede la possibilità per l'interessato di rivolgersi al Garante mediante un reclamo.

Quanto alle modalità, il successivo articolo 142 prevede che questo debba contenere un'indicazione, per quanto possibile dettagliata, dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonché gli estremi identificativi del titolare o del responsabile del trattamento, ove conosciuto.

Il Garante ha predisposto un modello per il reclamo, pubblicato nel proprio sito istituzionale, che di seguito si riporta.

**MODELLO DI RECLAMO\***

AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI  
P.ZZA VENEZIA, 11  
00187 ROMA

**Reclamo ex art. 77 del Regolamento (Ue) 2016/679 e artt. da 140-bis a 143 del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento**

*Il/La sottoscritto/a....., nato/a a .....il ....., residente in..... CF....., il/la quale ai fini del presente procedimento dichiara di voler ricevere eventuali comunicazioni al seguente recapito (indicare uno o più recapiti, tra indirizzo fisico, telefono, e-mail, fax) espone quanto segue:*

*(in questa parte del reclamo dovranno essere forniti necessariamente i seguenti elementi:)*

- a) dichiarazione in relazione alla circostanza che la Repubblica italiana è lo Stato membro in cui risiede abitualmente, lavora oppure il luogo ove si è verificata la presunta violazione;*
- b) gli estremi identificativi del titolare del trattamento (cioè, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali e che avrebbe commesso la violazione);*
- c) gli estremi identificativi del responsabile del trattamento (ove conosciuto);*
- d) un'indicazione, per quanto possibile dettagliata, dei fatti e delle circostanze su cui l'atto si fonda, ivi comprese eventuali richieste già rivolte sulla questione al Titolare del trattamento;*
- e) le disposizioni del Regolamento (Ue) 2016/679 e del Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento che si presumono violate, specificando se siano stati già eventualmente esercitati i diritti di cui agli artt. da 15 a 22 del Regolamento, e l'indicazione delle misure richieste.*

*Tutto ciò premesso, il/la sottoscritto/a:*

**CHIEDE**

*al Garante per la protezione dei dati personali, esaminato il reclamo che precede e ritenutane la fondatezza, di assumere nei confronti di .....(indicare il titolare del trattamento, recapito, ed ogni elemento utile alla sua individuazione) ogni opportuno provvedimento e, in particolare:*

- a) rivolgere a questi o al responsabile del trattamento avvertimenti o ammonimenti sul fatto che detti trattamenti possono verosimilmente violare, ovvero abbiano violato, le disposizioni vigenti in materia;*
- b) ingiungere al titolare del trattamento di soddisfare le richieste di esercizio dei diritti di cui agli artt. da 15 a 22 del Regolamento e/o di conformare i trattamenti alle disposizioni vigenti in materia anche nei confronti del responsabile del trattamento, ove previsto;*
- c) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento.*

*Elenco dei documenti allegati:*

- 1)
- 2)
- 3)

*Data*

*Firma*

*Si ricorda che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante), salvo che il fatto non costituisca più grave reato.*

*Modello di reclamo messo a disposizione dal Garante per la protezione dei dati personali, reperibile al seguente link: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4535524>.*

In base al successivo articolo 143 (come modificato dal decreto legislativo n. 101 del 2018), il Garante decide il reclamo entro nove mesi dalla data di presentazione e, in ogni caso, entro tre mesi dalla predetta data informa l'interessato sullo stato del procedimento. In presenza di motivate esigenze istruttorie, che il Garante comunica all'interessato, il reclamo è deciso entro dodici mesi. Avverso la decisione è ammesso ricorso giurisdizionale.

## **2.3 Le segnalazioni**

L'articolo 144 del Codice in materia di protezione dei dati personali prevede che chiunque può rivolgere una segnalazione che il Garante può valutare anche ai fini dell'emanazione dei provvedimenti di cui all'articolo 58 del GDPR, che possono essere adottati anche d'ufficio.

### **2.3.1 Il *revenge porn***

L'art. 144-*bis* del decreto legislativo n. 196 del 2003 dispone che chiunque, compresi i minori ultraquattordicenni, abbia fondato motivo di ritenere che registrazioni audio, immagini o video o altri documenti informatici a contenuto sessualmente esplicito che lo riguardano, destinati a rimanere privati, possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione attraverso piattaforme digitali senza il suo consenso, ha facoltà di segnalare il pericolo al Garante, il quale, nelle quarantotto ore dal ricevimento della segnalazione, decide ai sensi dei precedenti articoli 143 e 144.

Quando le registrazioni audio, le immagini o i video o gli altri documenti informatici riguardano minori, la segnalazione al Garante può essere effettuata anche dai genitori o dagli esercenti la responsabilità genitoriale o la tutela<sup>(219)</sup>.

I gestori delle piattaforme digitali destinatari dei provvedimenti del Garante conservano il materiale oggetto della segnalazione, a soli fini probatori e con misure indicate dal Garante, anche nell'ambito dei medesimi provvedimenti, idonee a impedire la diretta identificabilità degli interessati, per dodici mesi a decorrere dal ricevimento del provvedimento stesso.

Il Garante, con proprio provvedimento, può disciplinare specifiche modalità di svolgimento dei procedimenti in esame e le misure per impedire la diretta identificabilità degli interessati.

Quando il Garante, a seguito della segnalazione, acquisisce notizia della consumazione del reato di *revenge porn*, anche in forma tentata, nel caso di procedibilità d'ufficio trasmette al pubblico ministero la segnalazione ricevuta e la documentazione acquisita.

(219) L'invio al Garante di registrazioni audio, immagini o video o altri documenti informatici a contenuto sessualmente esplicito riguardanti soggetti terzi, effettuato dall'interessato, non integra il reato di cui all'articolo 612-ter del codice penale (*revenge porn*).

Questa è l'unica ipotesi – fa notare *Rosita Ponticiello*, coordinatrice del Dipartimento Pari opportunità dell'Unione Nazionale Camere Civili <sup>(220)</sup> – in cui si può chiedere la rimozione immediata delle immagini o dei video al Garante per la protezione dei dati personali senza aspettare il termine di un procedimento penale, quindi senza necessità di sporgere una denuncia o una querela.

### 2.3.2 Il regolamento del Garante n. 1 del 2019

L'articolo 33-*bis* (*Revenge porn*) del regolamento del Garante n. 1 del 4 aprile 2019 prevede che le segnalazioni di cui all'articolo 144-*bis* del Codice per la protezione dei dati personali, corredate delle registrazioni audio, immagini o video o altri documenti informatici a contenuto sessualmente esplicito, a sostegno delle stesse, sono presentate al Garante esclusivamente attraverso il modello, compilabile *on line*, pubblicato nell'apposita sezione del sito *web* istituzionale.

Il dipartimento, servizio o altra unità organizzativa competente, verificata la compatibilità della richiesta alla previsione di cui all'articolo 144-*bis* appena citato, entro 48 ore dal ricevimento della segnalazione, salva l'esigenza di acquisire un'integrazione delle informazioni fornite dal segnalante ai fini della predetta verifica, predispone il provvedimento volto ad impedire l'eventuale diffusione del materiale oggetto di segnalazione. Il provvedimento è adottato in via d'urgenza dal dirigente della medesima unità organizzativa e sottoposto a ratifica nella prima adunanza utile del Garante. In caso di mancata ratifica, il provvedimento decade.

Il provvedimento è trasmesso ai gestori delle piattaforme digitali, corredato del materiale oggetto di segnalazione o dalla relativa impronta hash.

### 2.4 *Deepfake*: la scheda informativa sui rischi dell'uso malevolo di questa nuova tecnologia

I *deepfake* sono foto, video e audio creati grazie a *software* di intelligenza artificiale (IA) che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce.

Il Garante per la protezione dei dati personali ha messo a punto una scheda informativa (qui di seguito riportata) per sensibilizzare gli utenti sui rischi connessi agli usi malevoli di questa nuova tecnologia, sempre più frequenti, anche a causa della diffusione di *app* e *software* che rendono possibile realizzare *deepfake*, anche molto ben elaborati e sofisticati, utilizzando un comune *smartphone*.

(220) Audizione del 17 novembre 2025.

Dicembre 2020

[www.gpdp.it](http://www.gpdp.it)**GPDP**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

# Deepfake

## Il falso che ti «ruba» la faccia (e la privacy)

### Cosa è un deepfake?

I **deepfake** sono foto, video e audio creati grazie a software di intelligenza artificiale (AI) che, partendo da contenuti reali (immagini e audio), riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce.

La parola deepfake è un neologismo nato dalla fusione dei termini “fake” (falso) e “deep learning”, una particolare tecnologia AI. Le tecniche usate dai deepfake sono simili a quelle delle varie app con cui ci si può divertire a modificare la morfologia del volto, a invecchiarlo, a fargli cambiare sesso, ecc.

La materia di partenza sono sempre i veri volti, i veri corpi e le vere voci delle persone, trasformati però in **“falsi” digitali**.

Le tecnologie deepfake, sviluppate come ausilio agli effetti speciali cinematografici, erano inizialmente molto costose e poco diffuse. Ma negli ultimi tempi hanno iniziato a diffondersi app e software che rendono possibile realizzare deepfake, anche molto ben elaborati e sofisticati, utilizzando un comune smartphone. La diffusione dei deepfake è di conseguenza notevolmente aumentata, e con essa i rischi connessi.

**GPDP**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**Deepfake**

Il falso che ti ruba la faccia (e la privacy)



## Il deepfake e il furto di identità

Quella realizzata con i deepfake è una forma particolarmente grave di **furto di identità**.

Le persone che compaiono in un deepfake a loro insaputa non solo subiscono una perdita di controllo sulla loro immagine, ma sono private anche del controllo sulle loro **idee e sui loro pensieri**, che possono essere **travisati** in base ai discorsi e ai comportamenti falsi che esprimono nei video.

Le persone presenti nei deepfake potrebbero inoltre essere **rappresentate in luoghi o contesti o con persone che non hanno mai frequentato o che non frequenterebbero mai**, oppure in situazioni che potrebbero apparire compromettenti.

In sostanza, quindi, un deepfake può ricostruire contesti e situazioni mai effettivamente avvenuti e, se ciò non è voluto dai diretti interessati, può rappresentare una grave minaccia per la riservatezza e la dignità delle persone.

**GPDP**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**Deepfake**

Il falso che ti ruba la faccia (e la privacy)



## I gravissimi rischi del deepnude

In particolari tipologie di deepfake, dette **deepnude**, persone ignare possono essere rappresentate nude, in pose discinte, situazioni compromettenti (ad esempio, a letto con presunti amanti) o addirittura in contesti pornografici. Con la tecnologia del deepnude, infatti, i visi delle persone (compresi soggetti minori) possono essere “innestati”, utilizzando appositi software, sui corpi di altri soggetti, nudi o impegnati in pose o atti di natura esplicitamente sessuale. E’ anche possibile prendere immagini di corpi vestiti e “spogliarli”, ricostruendo l’aspetto che avrebbe il corpo sotto gli indumenti e creando immagini altamente realistiche.

Inizialmente il fenomeno ha coinvolto personaggi famosi allo scopo di screditarli o ricattarli. Ma negli ultimi tempi, con la sempre maggiore diffusione di software che utilizzano questa tecnologia, il rischio coinvolge anche persone comuni, le quali possono diventare oggetto di azioni psicologicamente e socialmente molto dannose. Come, ad esempio, il “**revenge porn**”, cioè la condivisione online - a scopo di ricatto, denigrazione o vendetta, da parte di ex partner, amanti o spasimanti respinti - di foto e video a contenuto sessuale o addirittura pornografico, che, nel caso del deepnude, sono ovviamente falsi.

Video deepnude possono essere utilizzati, a totale insaputa dei soggetti rappresentati nelle immagini, anche per alimentare la pratica del **sexting** (cioè lo scambio e diffusione di immagini di nudo, che a volte coinvolge anche soggetti minori), la **pornografia illegale** e, purtroppo, anche reati gravissimi come la **pedopornografia**.

[www.gpdp.it](http://www.gpdp.it)

**GPDP**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**Deepfake**

Il falso che ti ruba la faccia (e la privacy)



## Deepfake e cyberbullismo

**I video deepfake possono essere creati ad hoc per realizzare veri e propri atti di cyberbullismo, che hanno come vittime soprattutto giovani.**

Un deepfake può essere realizzato per denigrare, irridere e screditare le persone coinvolte, o addirittura per ricattarle, chiedendo soldi o altro in cambio della mancata diffusione del video oppure per la sua cancellazione se è già stato diffuso.

## Deepfake e fake news

**I deepfake possono riguardare politici o opinion leader, con lo scopo di influenzare l'opinione pubblica.** Video deepfake possono ad esempio essere mostrati o inviati agli elettori che simpatizzano per un determinato personaggio politico, rappresentandolo mentre compie azioni poco lecite o mentre si trova in situazioni sconvenienti, allo scopo di screditarlo ed **influenzare le opinioni o il voto**. In questo modo, i deepfake possono purtroppo contribuire alla diffusione di fake news e alla disinformazione.

Il deepfake può quindi arrivare a privare le persone della cosiddetta "autodeterminazione informativa" ("ciò che voglio far sapere di me lo decido io"), come pure ad incidere sulla loro libertà decisionale ("quello che penso e faccio è una scelta su cui gli altri non possono interferire").

[www.gpdp.it](http://www.gpdp.it)

**GPDP**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**Deepfake**

Il falso che ti ruba la faccia (e la privacy)



## Deepfake e cybercrime

Il deepfake può essere utilizzato per attività telematiche illecite, come lo spoofing (il furto di informazioni che avviene attraverso la falsificazione di identità di persone o dispositivi, in modo da ingannare altre persone o dispositivi e ottenere la trasmissione di dati), il phishing e il ransomware.

**Volti e voci artefatti possono essere utilizzati per ingannare i sistemi di sicurezza basati su dati biometrici vocali e facciali.**

Ad esempio, video o audio-messaggi deepfake creati da malintenzionati possono essere inviati ai nostri colleghi, amici o parenti **per invitarli a cliccare su link o aprire allegati a messaggi** che espongono pc, smartphone o altri dispositivi e sistemi a pericolose intrusioni, oppure per convincerli a fornire, ingannando la loro fiducia, informazioni e dati sensibili. Inoltre oggi molti sistemi digitali (domotica, assistenti vocali, smartphone, nonché alcuni sistemi bancari o sanitari) ricorrono a **dati biometrici vocali e facciali come sistema di autenticazione per l'accesso**. Video e audio-messaggi deepfake potrebbero essere utilizzati per **ingannare** tali sistemi.

Anche se al momento il livello avanzato delle tecnologie di sicurezza e la ancora relativa imprecisione dei deepfake stanno limitando questi fenomeni, l'attenzione deve essere comunque alta.

**GPDP**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**Deepfake**

Il falso che ti ruba la faccia (e la privacy)

## Come proteggersi dai deepfake

Le grandi imprese del digitale (piattaforme social media, motori di ricerca, ecc.) stanno già studiando e applicando delle **metodologie per il contrasto al fenomeno**, come algoritmi di intelligenza artificiale capaci di individuare i deepfake o sistemi per le segnalazioni da parte degli utenti, e stanno formando team specializzati nel monitoraggio e contrasto al deepfake. E le **Autorità di protezione dei dati personali** possono intervenire per prevenire e sanzionare le violazioni della normativa in materia di protezione dati.

Tuttavia, **il primo e più efficace strumento di difesa è rappresentato sempre dalla responsabilità e dall'attenzione degli utenti. Ecco allora alcuni suggerimenti:**

- ☐ **Evitare di diffondere in modo incontrollato immagini personali o dei propri cari.** In particolare, se si postano immagini sui social media, è bene ricordare che le stesse potrebbero rimanere online per sempre o che, anche nel caso in cui si decida poi di cancellarle, qualcuno potrebbe già essersene appropriato.
- ☐ Anche se non è semplice, **si può imparare a riconoscere un deepfake.** Ci sono elementi che aiutano: l'immagine può apparire pixellata (cioè un pò "sgranata" o sfocata); gli occhi delle persone possono muoversi a volte in modo innaturale; la bocca può apparire deformata o troppo grande mentre la persona dice alcune cose; la luce e le ombre sul viso possono apparire anormali.
- ☐ **Se si ha il dubbio che un video o un audio siano un deepfake realizzato all'insaputa dell'interessato, occorre assolutamente evitare di condividerlo** (per non moltiplicare il danno alle persone con la sua diffusione incontrollata). E si può magari decidere di segnalarlo come possibile falso alla piattaforma che lo ospita (ad esempio, un social media).
- ☐ **Se si ritiene che il deepfake sia stato utilizzato in modo da compiere un reato o una violazione della privacy**, ci si può rivolgere, a seconda dei casi, alle autorità di polizia (ad esempio, alla Polizia postale) o al **Garante per la protezione dei dati personali**.

#### 2.4.1 *Deepnude*: il provvedimento n. 789 del 18 dicembre 2025

Il Garante per la protezione dei dati personali ha adottato un provvedimento di avvertimento nei confronti degli utilizzatori di servizi basati sull'intelligenza artificiale, come *Grok*, *ChatGPT* e *Clothoff* – quest'ultima piattaforma già destinataria di un provvedimento di blocco nell'ottobre 2025 – e altri servizi analoghi disponibili *on line*, che consentono di generare e condividere contenuti a partire da immagini o voci reali, arrivando anche a « spogliare » persone senza il loro consenso.

L'Autorità ricorda che l'utilizzo di tali strumenti e la diffusione dei contenuti così generati, tramite *social media* o altri servizi digitali e applicazioni di messaggistica, possono determinare – oltre a possibili fattispecie di reato, in assenza del consenso degli interessati – gravi violazioni dei diritti e delle libertà fondamentali delle persone coinvolte, con tutte le conseguenze, anche sanzionatorie, previste dalla normativa europea in materia di protezione dei dati personali.

Nello specifico, il Garante, a seguito di un'attività istruttoria avviata d'ufficio, ha riscontrato la presenza sul mercato di numerosi servizi che consentono agli utenti di utilizzare la voce o le immagini anche di terze persone – personaggi noti e non – per la generazione di contenuti audio, fotografici e/o audiovisivi basati su tali voci o immagini.

Tali servizi di generazione artificiale di contenuti in molti casi consentono agli utenti anche di condividere i contenuti così realizzati attraverso le principali piattaforme *social*.

La tecnologia sulla quale tali servizi sono basati è uno strumento che si avvale dell'intelligenza artificiale per la generazione di contenuti multimediali digitali, audio o video idonei a manipolare la realtà (*deepfake*); più precisamente, alle persone a cui appartengono le voci e le immagini utilizzate nei *deepfake* sopra descritti possono essere attribuite idee e pensieri rappresentati con la loro voce parlata e le loro immagini senza che ciò corrisponda effettivamente alla loro volontà e coscienza.

Il *deepfake* può privare le persone della propria « autodeterminazione informativa » (« *ciò che voglio far sapere di me lo decido io* ») e incidere sulla loro libertà decisionale (« *quello che penso e faccio è una scelta su cui gli altri non possono interferire* »).

Il funzionamento di tali servizi sottende il trattamento di dati di natura personale, segnatamente della voce e/o delle immagini, che potrebbero essere riferiti a soggetti terzi rispetto all'utilizzatore del servizio medesimo, i quali potrebbero non essere a conoscenza del trattamento dei loro dati personali <sup>(221)</sup>.

La voce e le immagini di una persona rientrano nella definizione di cui all'articolo 4 punto 1) del GDPR, che definisce « dato personale » « *qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identifica-*

(221) Il Regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi, con la esclusione dei trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

zione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale ».

La voce e le immagini, dunque, possono certamente rientrare fra i cosiddetti identificatori, ovvero quella categoria di informazioni che hanno un rapporto diretto con la persona identificata<sup>(222)</sup> e, dunque, tale identificatore vocale o visivo può essere classificato nella categoria dei dati di tipo biometrico se ricorrono alcuni criteri specifici.

Questi consistono nella natura del dato, che deve essere riferito a una caratteristica fisica, fisiologica o comportamentale di una persona, e ai mezzi e finalità del trattamento svolto che devono consistere in un trattamento tecnico con scopo di identificazione univoca<sup>(223)</sup>; in questo caso è, pertanto, necessario non solo verificare la sussistenza di una base giuridica ai sensi dell'articolo 6 del GDPR, ma anche di una delle condizioni indicate dall'articolo 9.2 del GDPR. Condizione necessaria anche nell'ipotesi in cui la voce possa rientrare nel novero delle categorie particolari di dati.

Ai sensi del considerando 39 del GDPR, «È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali» e, nel caso dei *deepfake*, tale esigenza risulta indifferibile in ragione della presenza di rischi elevati connessi al trattamento di dati personali, segnatamente della voce, riferibili a soggetti terzi, che, verosimilmente, non sono informati del trattamento medesimo.

I rischi elevati connessi al trattamento in argomento appaiono ulteriormente amplificati in considerazione del potenziale utilizzo dei dati artefatti elaborati mediante strumenti di intelligenza artificiale per scopi giuridicamente rilevanti, come l'uso ingannevole finalizzato alla frode, ovvero la diffamazione e la sostituzione di persona.

In base al Considerando 75 del GDPR, i «rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano ».

I fornitori dei servizi di generazione di contenuti artificiali basati sull'utilizzo di voci o immagini di terzi, sin dalla fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, nel tenere conto del diritto alla protezione dei dati, devono considerare lo stato dell'arte, impegnandosi a far sì che

(222) I dati in forma di suoni e immagini costituiscono dati personali in quanto possono rappresentare informazioni su una persona (*Opinion 4/2007 on the concept of personal data* – WP136)

(223) I «dati biometrici» sono i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici (articolo 4.1 n. 14 del GDPR).

i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati (Considerando 78 e articolo 25 del GDPR).

Sulla scorta di queste argomentazioni, il Garante ha avvertito tutte le persone fisiche o giuridiche che utilizzano, in qualità di titolari o di responsabili del trattamento, servizi di generazione di contenuti basati sull'intelligenza artificiale partendo da voci o immagini reali di terze persone, che tale trattamento dei dati personali, qualora sia effettuato in assenza di un'idonea condizione di liceità e senza che siano preliminarmente fornite agli interessati informazioni corrette e trasparenti, può, verosimilmente, violare le disposizioni del GDPR (in particolare gli articoli 5, paragrafo 1, lettera a), 6 e 9), con tutte le conseguenze, anche di carattere sanzionatorio, previste dalla disciplina in materia di protezione dei dati personali.

## 2.5 I limiti di tutela

Gli strumenti indicati non colpiscono pienamente la produzione e la condivisione organizzata di contenuti generati o alterati con sistemi di intelligenza artificiale, cosiddetti «*deep fake*», e non risolvono i «*colli di bottiglia*» per quanto concerne la rimozione rapida dei contenuti e la garanzia della loro mancata reimmissione, c.d. «*stay down*», nelle piattaforme digitali e nei siti internet esteri. A livello dell'Unione europea, il *Digital Services Act* (Regolamento 2022/2065/UE) è pienamente in vigore dal 17 febbraio 2024 e in Italia il coordinatore dei servizi digitali è l'AGCOM, che ha pubblicato la prima relazione delle proprie attività nel 2025. Il citato Regolamento attribuisce la facoltà di emanare ordini di rimozione da parte delle autorità competenti e prevede canali di segnalazione, cosiddetti «*notice & action*», più efficaci, compresi i segnalatori certificati, cosiddetti «*trusted flaggers*», con sanzioni fino al 6 per cento del fatturato globale in caso di inadempimento.

Il 13 giugno 2024 è stato approvato il Regolamento 2024/1689/UE, che stabilisce regole armonizzate sull'intelligenza artificiale, c.d. «*AI Act*», applicabile a decorrere dal 2 agosto 2026, nel quale si prevedono obblighi di trasparenza e di etichettatura per i contenuti generati o manipolati dall'intelligenza artificiale che costituiscono un *deep fake* (articolo 50). Tuttavia, tale normativa non penalizza di per sé la produzione non consensuale di contenuti sessualmente espliciti generati o alterati con sistemi di intelligenza artificiale, né definisce procedure di rimozione rapida: serve dunque un coordinamento nazionale che integri le disposizioni del *Digital Services Act* e dell'*AI Act* con quelle nazionali, prevedendo illeciti penali e civili specifici nonché procedure di esecuzione rapide.

Per quanto concerne la prevenzione e la rimozione dei contenuti, si richiamano iniziative come il sito internet *StopNCII.org*, basate su tecnologie, cosiddette «*hash matching*», per il riconoscimento dei contenuti intimi non consensuali, oggi adottate dalle principali piattaforme digitali, tra cui Meta, ma manca un polo nazionale che integri tali tecnologie in modo obbligatorio e interoperabile con le autorità italiane.

### 3. L'Agenzia per la Cybersicurezza Nazionale (ACN)

#### 3.1 La natura e le funzioni

L'Agenzia per la Cybersicurezza Nazionale (ACN) è stata istituita con decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni dalla legge 4 agosto 2021, n. 109, che ha ridefinito l'architettura nazionale della cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.

L'Agenzia ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico. Si occupa di prevenire e mitigare il maggior numero di attacchi cibernetici e di favorire il raggiungimento dell'autonomia tecnologica. Tra i principali compiti dell'Agenzia c'è l'attuazione della Strategia Nazionale di Cybersicurezza, adottata dal Presidente del Consiglio dei ministri, che contiene gli obiettivi da perseguire entro il 2026.

Come spiegato dal Direttore, il Prefetto *Bruno Frattasi* <sup>(224)</sup>, la cybersicurezza nazionale è una materia il cui compito primario è quello di garantire la resilienza sistemica del Paese. Per «resilienza sistemica» si intende la protezione delle infrastrutture del Paese, innanzitutto di quelle strategiche, a cui è legata la continuità della vita ordinaria del nostro Paese, della nostra nazione.

L'Agenzia non è un organo di polizia giudiziaria ma interviene a supporto dei soggetti la cui sicurezza viene messa a repentaglio, avendo conoscenza della minaccia attraverso l'acquisizione di informazioni grazie alle piattaforme di *threat intelligence* a cui aderisce, che la mettono nelle condizioni di poter percepire e capire quali sono i segnali, anche deboli, della minaccia *web* che può muovere verso il Paese. Naturalmente può capitare che la minaccia possa essere indirizzata, sotto forma di violenza digitale, contro una donna, un minore, un soggetto fragile o vulnerabile.

L'azione della Agenzia viene integrata dall'attività delle forze di polizia, in particolare della Polizia postale e del CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche), che si confronta con il *cybercrime*, ovvero con l'attacco criminale alle reti, ai sistemi, ai servizi, ma anche alla stessa protezione dei dispositivi, individuali e personali, che possono essere oggetto di aggressione di vario tipo, con riferimento soprattutto all'integrità, alla confidenzialità e alla disponibilità dei dati.

Quello che accomuna l'insieme di queste azioni è proprio la protezione del dato, dell'informazione. Questo vale per le infrastrutture nazionali, che ospitano una rilevante mole di dati relativi alla sicurezza economico-finanziaria ed energetica del Paese, ma vale anche per le persone e gli individui che, naturalmente, ospitano sui propri dispositivi un patrimonio di informazioni che riguarda le loro vite, i modi di atteggiarsi rispetto al mondo circostante e all'esterno, gli affetti, i gusti, le inclinazioni sessuali, le opinioni ideologico-politiche: la sfera personale.

(224) Audizione del 6 novembre 2025.

Tutti viviamo ormai in una condizione di quasi indistinzione tra la realtà fisica e la realtà digitale e virtuale. Distinguiamo l'*off line* dall'*on line* il cui incrocio descrive la realtà che stiamo vivendo, una realtà ibrida, la c.d. *on life*<sup>(225)</sup>, la vita in rete.

### 3.2 La consapevolezza del rischio digitale

Una delle dorsali fondamentali della strategia nazionale del piano di implementazione della cybersicurezza del nostro Paese è data dalla formazione delle competenze digitali e dalla consapevolezza dei rischi digitali.

La consapevolezza del rischio digitale non è soltanto indirizzata ai soggetti pubblici e privati che hanno da difendere un loro patrimonio professionale o amministrativo ma anche ai cittadini.

Particolarmente esposti a questo rischio sono proprio i giovani e gli adolescenti, il che sembra quasi controintuitivo: di norma viene associata l'idea della capacità digitale ai giovani, in quanto nativi digitali, ma questo è un po' un luogo comune, una petizione di principio, perché in realtà proprio i giovani adolescenti – che sicuramente hanno capacità digitali più avanzate rispetto alla fascia media della popolazione nazionale – tuttavia hanno anche un'incompetenza nell'uso dei mezzi digitali rispetto ai fini di certe attività digitali che si svolgono nel *web*.

Occorre lavorare su una maggiore consapevolezza dei più giovani verso il « rischio *cyber* » così da renderli più avveduti nell'uso dei mezzi digitali con un « senso di cittadinanza digitale » che significa una maggiore maturità nel loro uso.

L'Agenzia ha sottoscritto, nel mese di dicembre 2024, un accordo con il Ministero dell'istruzione e del merito perché si introducano nei cicli scolastici, di ogni ordine e grado, finanche alle elementari, pillole di « educazione digitale »<sup>(226)</sup>.

L'introduzione di elementi di educazione digitale non è tesa soltanto a professionalizzare l'uso del mezzo digitale<sup>(227)</sup>. Lo scopo è

(225) Neologismo d'autore, creato dal filosofo italiano Luciano Floridi giocando sui termini *on line* ('in linea') e *off line* ('non in linea'): *on life* è quanto accade e si fa mentre la vita scorre, restando collegati a dispositivi interattivi (*on + life*). La dimensione vitale, relazionale, sociale e comunicativa, lavorativa ed economica, vista come frutto di una continua interazione tra la realtà materiale e analogica e la realtà virtuale e interattiva. Di *on life* parla anche Marina Terragni, Garante per l'Infanzia e l'Adolescenza, nella relazione trasmessa a questa Commissione in data 9 febbraio 2026.

(226) Il protocollo d'intesa per promuovere l'educazione informatica e cibernetica nelle scuole prevede una serie di iniziative rivolte a studenti, docenti e genitori, con l'obiettivo di diffondere la cultura della sicurezza digitale a livello nazionale. Il protocollo si focalizza su diversi aspetti cruciali: la consapevolezza dei rischi digitali (cyberbullismo, contenuti inappropriati, minacce alla *privacy*), l'acquisizione di competenze di *cybersafety* e igiene digitale, la promozione della cittadinanza digitale e l'orientamento verso le discipline STEM (*Science, Technology, Engineering, Mathematics*), con particolare attenzione alla sicurezza informatica. Previsti, inoltre, percorsi di formazione continua per i docenti, la creazione di materiali didattici innovativi e l'integrazione delle tematiche di cybersicurezza nei Piani dell'Offerta Formativa (POF) delle scuole.

(227) Sappiamo che nell'età dello sviluppo c'è la necessità di uniformarsi al branco e sappiamo che c'è una spinta all'adattamento di stereotipi, quindi un bisogno di accettazione, che può portare anche ad accettare certi tipi di richieste *on line*. C'è una fragilità intrinseca sia nei bambini che nelle bambine, in quanto piccoli, in età dello sviluppo, una particolare sensibilità al *victim blaming* e un particolare timore

fare in modo che gli adolescenti possano avere, nei confronti del mezzo digitale, una « postura » di responsabilità che li porti a capire che nel mondo digitale non c'è soltanto da divertirsi, ma anche da confrontarsi con un rischio, con dei pericoli che suggeriscono cautela<sup>(228)</sup>.

### 3.2.1 Le tecnologie *disruptive*

La situazione rischia di aggravarsi per effetto della introduzione delle tecnologie *disruptive*<sup>(229)</sup> nel nostro tempo. Il riferimento è, in particolare, all'intelligenza artificiale che oggi rappresenta una potente arma di rafforzamento della minaccia cibernetica.

Ciò è emerso in tutta la sua portata nei recenti casi di donne messe alla gogna mediatica attraverso l'esposizione dei loro corpi, fatta in maniera oscena, attraverso l'uso – *rectius* l'abuso – dell'intelligenza artificiale.

La risposta del nostro Paese, tuttavia, è arrivata, ancora una volta, in termini securitari.

alla vittimizzazione secondaria anche da parte della famiglia. Questo può portare i minori, anche nel caso in cui siano già esposti a situazioni di disagio, se non di violenza *on line*, a nasconderle perché temono gli effetti sia su di loro che sulla loro famiglia (Rosanna Milone, responsabile progetti e *Awareness and Advocacy Strategist* della Fondazione Carolina, audizione del 24 novembre 2025).

(228) Per Barbara Leda Kenny, *Senior Gender Expert* della Fondazione G. Brodolini (audizione del 22 ottobre 2025), una fascia di età alla quale occorre prestare particolare attenzione è quella da 11 a 14 anni. I preadolescenti. Secondo lo studio di Chayn Italia sulla violenza digitale, è questa la fascia di età in cui le ragazze si sentono più esposte alla violenza. Secondo la *Internet Watch Foundation*, le bambine tra 11 e 13 anni sono le più vulnerabili all'abuso sessuale *on line*. Il dato inquietante è che quasi la metà dei materiali di abuso identificati in rete è stata autoprodotta dalle ragazze stesse, spesso sotto ricatto o minaccia, nell'80% dei casi proprio da ragazzine di questa fascia di età. Le preadolescenti entrano negli spazi digitali senza mediazione, spesso senza sorveglianza e senza strumenti per riconoscere i pericoli, vivono in un *continuum* che è stato definito « *long life* »: passano circa quattro ore al giorno del loro tempo in rete e l'85% di loro riceve uno smartphone prima di compiere 11 anni. Mentre a quell'età la socialità reale è mediata dagli adulti, nella vita *on line* non lo è. Non solo, a complicare questo scenario c'è un dato particolare, evidenziato da un centro di ricerca americano molto prestigioso che si chiama *Pew Research Center*: le preadolescenti e i loro genitori non utilizzano gli stessi strumenti quando si parla di ambienti digitali. Usano altre *chat*, usano altre applicazioni, altre piattaforme, che i genitori non conoscono e non sanno utilizzare. Come rilevato da Barbara Poggio, componente del comitato scientifico della Fondazione Giulia Cecchettin (audizione dell'11 novembre 2025), le famiglie spesso non hanno la capacità e non sono neanche in grado di sapere che cosa passa sui computer o sui cellulari dei loro figli. Sappiamo che oggi – ce lo dicono molte ricerche – il primo accesso alla sessualità avviene non più, come una volta, nelle reti amicali, ma attraverso i *social*, ed è un accesso molto problematico. Non sono *tutorial* fatti da esperti che spiegano come funziona, ma sono video estremamente violenti, a volte sono stupri, che magari passano su *Telegram* o anche in gruppi protetti da altri sguardi. Le famiglie spesso non lo sanno, perché i ragazzi fanno queste cose nelle loro stanze, con gli amici. Secondo Cristina Obber, scrittrice e giornalista, audita il 10 novembre 2025, i ragazzi e le ragazze manifestano paura rispetto alla violenza però, nel contempo, continuano a utilizzare i dispositivi con una certa superficialità e senza la consapevolezza che, a volte, alcune condotte ormai normalizzate sono reati, come il *sexting* (invio volontario di immagini intime nelle chat private tra minori).

(229) L'espressione « *disruptive innovation* » appare per la prima volta in letteratura in un articolo di Clayton Christensen e Joseph Bower, « *Disruptive technologies: catching the wave* », pubblicato nel 1995 sull'*Harvard Business Review*. La traduzione letterale del termine « *disruptive* » è « dirompente », « devastante », « distruttivo » e fa riferimento a tutte quelle innovazioni capaci di rivoluzionare un modello di *business* preesistente ridefinendo i confini dell'arena competitiva e stravolgendo il modo in cui i consumatori sono abituati a utilizzare prodotti e servizi.

La legge 23 settembre 2025, n. 132, ha colpito il fenomeno del *deepfake* dal punto di vista penale, introducendo una nuova fattispecie di reato, con una pena da uno a cinque anni (articolo 612-*quater* del codice penale); la minaccia della sanzione penale — ha concluso il prefetto *Bruno Frattasi* — non può essere l'unica forma di risposta a questo tipo di evento.

## Parte VII LE TUTELE PROCESSUALI

### 1. Il processo civile

#### 1.1 La tutela cautelare d'urgenza

Considerata l'urgenza di inibire l'attività di diffusione di immagini, audio o video, reali o generati con l'intelligenza artificiale, lesivi della dignità delle persone coinvolte, diventa fondamentale il ricorso allo strumento della tutela cautelare predisposto dal sistema processuale civile.

Il tribunale, adito ex articolo 700 del codice di procedura civile, oltre a ordinare l'immediata cessazione e rimozione di tutte le pubblicazioni a contenuto ingiurioso e diffamatorio può, su richiesta della parte istante, prevedere la corresponsione di una somma di denaro per ogni violazione o inosservanza dell'ordine nonché per ogni giorno di ritardo nell'esecuzione del provvedimento <sup>(230)</sup>.

Questo rimedio cautelare atipico è finalizzato ad apprestare tutela al diritto – che il ricorrente intende far valere in giudizio, qualora sia minacciato, nel tempo (anche non breve) della tutela ordinaria, da un « *pregiudizio imminente ed irreparabile* » – mediante l'emanazione dei provvedimenti che appaiano più idonei « *ad assicurare provvisoriamente gli effetti della decisione* ». Esso mira, in concreto, ad evitare che la durata del processo instaurato possa andare a detrimento della parte, precludendo o vanificando l'effettività della tutela giurisdizionale azionata in via ordinaria <sup>(231)</sup>.

Il primo dei presupposti, cui si àncora la tutela sommaria è, secondo le regole generali della funzione cautelare, il *periculum in mora*, da intendersi come attualità, imminenza e irreparabilità del pregiudizio. Irreparabile è ciò che, per sua natura, non è risarcibile per equivalente, ovvero, tradizionalmente, tutti i diritti della persona o assoluti, ma anche i diritti e le facoltà collegati a uno *status*, ovvero posizioni giuridiche relativamente alle quali il ristoro monetario si appalesi impossibile o semplicemente insufficiente o, comunque, non integralmente ripristinatorio <sup>(232)</sup>.

Il secondo presupposto è il *fumus boni iuris* della domanda, ovvero la valutazione, allo stato degli atti e compatibilmente con la cognizione sommaria rimessa alla fase cautelare, della sua fondatezza.

(230) Si tratta delle misure di coercizione indiretta previste dall'articolo 614-bis del codice di procedura civile, introdotto dalla legge 18 giugno 2009, n. 69, sul modello dell'istituto di origine francese (con funzione indennitaria a beneficio del creditore) dell'*astreinte*.

(231) Cfr., *ex multis*, Cass. civ., sez. II n. 4964 del 2004.

(232) Tale pregiudizio deve rivestire una duplice connotazione: precisamente, dal punto di vista temporale, deve trattarsi di un pregiudizio imminente, ovvero che rischierebbe di avverarsi durante il tempo occorrente per la tutela ordinaria del diritto; la situazione di pericolo per il diritto deve essere oggettiva, reale ed attuale; dal punto di vista contenutistico, deve trattarsi di un pregiudizio irreparabile, ovvero che non sia integralmente rimediabile con le tecniche risarcitorie per equivalente o con gli strumenti di reintegrazione in forma specifica.

In caso di pubblicazione di post o commenti offensivi su *social network* sussistono, invero, tutti presupposti per la tutela d'urgenza:

a) la lesione di un diritto della personalità costituzionalmente garantito, condotta che tra l'altro integra il reato di diffamazione (*fumus boni iuris*);

b) il possibile pregiudizio che possa derivare al suddetto diritto nelle more del giudizio ordinario e, quindi, il fondato e attuale timore che il diritto sia esposto ad un pericolo imminente e irreparabile (*periculum in mora*);

c) l'inesistenza di una misura cautelare tipica atta a garantire l'effettività della tutela (residualità).

## 1.2 Il risarcimento del danno

La tutela cautelare atipica non può essere invocata per ottenere il risarcimento del danno, che potrà essere richiesto solo nel corso del giudizio ordinario di cognizione, anche ai sensi dell'articolo 2059 del codice civile (Danni non patrimoniali).

Il danno non patrimoniale, derivante dalla lesione di diritti inviolabili della persona, come tali costituzionalmente garantiti, è risarcibile – sulla base di una interpretazione costituzionalmente orientata dell'articolo 2059, e al di là delle ipotesi di danno derivante dalla commissione di reato, o dei casi in cui la legge consente espressamente il ristoro dei pregiudizi non patrimoniali – a tre condizioni:

a) che l'interesse leso (e non il pregiudizio sofferto) abbia rilevanza costituzionale;

b) che la lesione dell'interesse sia grave, nel senso che l'offesa superi una soglia minima di tollerabilità (in quanto il dovere di solidarietà, di cui all'articolo 2 della Costituzione, impone a ciascuno di tollerare le minime intrusioni nella propria sfera personale inevitabilmente scaturenti dalla convivenza);

c) che il danno non sia futile, vale a dire che non consista in meri disagi o fastidi, ovvero nella lesione di diritti del tutto immaginari, come quello alla qualità della vita o alla felicità, dovendo ritenersi palesemente non meritevoli di tutela risarcitoria i pregiudizi consistenti in detti disagi, fastidi, disappunti, ansie e in ogni altro tipo di insoddisfazione concernente gli aspetti più disparati della vita<sup>(233)</sup>.

Rosaria Filloramo, referente del Dipartimento Pari opportunità dell'Unione Nazionale Camere Civili<sup>(234)</sup>, ha spiegato che, quando si parla di risarcimento del danno e, quindi, di profilo economico, abbiamo una grossa lacuna nell'ambito della violenza di genere: l'assenza di parametri di riferimento. Abbiamo semplicemente delle tabelle in sede civile, che sono le tabelle a cui normalmente si fa riferimento in sede di quantificazione del danno da incidenti stradali.

(233) Cass. civ., sez. un., 11 novembre 2008, n. 26972.

(234) Audizione del 17 novembre 2025.

La violenza digitale è fonte di danno non patrimoniale sotto tre aspetti: il danno biologico, il danno morale e il danno esistenziale. In tutti e tre i profili non c'è, effettivamente, un parametro di riferimento oggettivo cui il giudice di merito possa far riferimento per poter risarcire la vittima del grave danno che subisce, un danno permanente come nessun altro. Ovviamente, questo è importante soprattutto se si tiene conto che, in materia, manca una disciplina del danno punitivo per l'autore della condotta illecita, con funzione di deterrenza<sup>(235)</sup>.

### 1.3 La c.d. *class action*

L'azione di classe costituisce un meccanismo diffuso di tutela dei diritti di consumatori che consente di gestire, in un unico procedimento, molteplici richieste di risarcimento derivanti da uno stesso illecito, lesivo di una pluralità di situazioni soggettive.

Attraverso la c.d. *class action*, la stessa tutela che ogni individuo potrebbe teoricamente esercitare singolarmente può essere esercitata collettivamente grazie all'omogeneità delle situazioni e all'appartenenza alla stessa categoria di consumatori.

L'azione – disciplinata dagli articoli 840-*bis* e seguenti del codice di procedura civile – può essere esercitata per ottenere il risarcimento del danno derivante dalle condotte offensive o lesive della dignità delle persone (come nel caso della pubblicazione di immagini, video o commenti offensivi).

Ai fini del riconoscimento della fondatezza della domanda avente a oggetto il risarcimento del danno non patrimoniale proposta nelle forme processuali dell'azione di classe, spetta al giudice di merito coordinare l'indagine condotta sulla serietà e la gravità dell'offesa inferta all'interesse costituzionalmente protetto, con le esigenze proprie dell'azione di classe disegnata dal legislatore italiano, con particolare riguardo alla necessità che le situazioni soggettive lese e i diritti concretamente pregiudicati (di necessaria rilevanza costituzionale) siano caratterizzati (non solo dalla gravità e serietà della relativa lesione, bensì anche) dall'essenziale requisito della relativa omogeneità, inteso, quest'ultimo, come il tratto proprio di pretese individuali che, vantate da un insieme di consumatori o di utenti, siano accomunate da caratteristiche tali da giustificarne un apprezzamento seriale e una gestione processuale congiunta, dovendo escludersi, sul piano logico, prima ancora che su quello giuridico, la compatibilità dello strumento processuale così delineato dal legislatore con l'esecuzione di accertamenti calibrati su specifiche situazioni personali o con valutazioni che

(235) La disciplina della responsabilità per colpa, traibile dalla formulazione dell'articolo 2043 del codice civile, non delinea un modello puramente preventivo-sanzionatorio, recando una componente anche compensativa che giustifica l'impossibilità di accordare un risarcimento del danno superiore a quello effettivamente patito e dimostrato dal danneggiato. In dottrina, l'orientamento predominante, muovendo da un inequivoco dato normativo – articolo 1223 del codice civile al quale rinvia l'articolo 2056 –, indica il limite invalicabile della sanzione: il danno non può essere risarcito in misura variabile onde colpire in misura adeguata atteggiamenti particolarmente riprovevoli ovvero evitare locupletazioni. Nel nostro ordinamento privatistico è opinione comune quella secondo cui non si sia affermata, quanto meno in termini di istituto di dignità generale, la figura della cosiddetta pena privata, la cui intensità, sul modello statunitense dei *punitive damages*, andrebbe rapportata agli elementi di cui all'articolo 133 del codice penale, con particolare riguardo al profitto economico tratto dal danneggiante.

si soffermino sulla consistenza specifica della sfera emotiva o dell'esperienza dinamico-relazionale di singoli danneggiati. Nei casi in cui, infatti, le doglianze dei danneggiati siano tali da non lasciare prefigurare la possibilità di una valutazione tendenzialmente standardizzata anche delle relative conseguenze pregiudizievoli (sia per quel che specificamente riguarda l'*an* che il *quantum* del danno), il meccanismo della tutela di classe deve ritenersi per ciò stesso impraticabile.

Lungi dall'escludere in astratto la compatibilità del risarcimento del danno non patrimoniale con il ricorso alle forme processuali dell'azione di classe (una soluzione, per vero drastica, pur sostenuta da talune voci della letteratura specialistica), l'azione di classe rimane pur sempre compatibile con la rivendicazione della tutela risarcitoria dei danni non patrimoniali là dove di questi ultimi siano tuttavia posti rigorosamente in risalto i tratti in qualche modo comuni a tutti i membri della classe (purché adeguatamente specificati e comprovati), con la conseguenza che l'originario proponente ha l'onere di domandare la riparazione di un danno non patrimoniale che non sia individualizzato, ma sia fondato su circostanze comuni a tutti i membri della classe <sup>(236)</sup>.

In ciascuna di tali ipotesi, tuttavia, sarà in ogni caso necessaria la precisa identificazione delle situazioni soggettive lese, della qualità della relativa protezione a livello costituzionale (fuori dai casi di danni non patrimoniali da reato o da tipizzazione legislativa del fatto) e dei termini concreti dell'effettiva serietà e gravità delle lesioni inferte e dei pregiudizi subiti, non confondibili con meri disagi, fastidi, disappunti, ansie o con ogni altro tipo di insoddisfazione concernente gli aspetti più disparati della vita, al fine di scongiurare un'inammissibile declinazione in chiave punitiva della responsabilità risarcitoria, in assenza di indici legislativi suscettibili di giustificarla <sup>(237)</sup>.

(236) Una simile soluzione (nella misura in cui esclude l'obbligo di personalizzazione del danno non patrimoniale nell'ambito dell'azione di classe) ha il pregio di prefigurare la possibilità, per ciascun singolo danneggiato, di scegliere liberamente se promuovere o aderire a un'azione di classe (rinunciando a un'istruttoria individuale e accettando di fatto un risarcimento forfettizzato), ovvero promuovere un'azione individuale insistendo per una liquidazione personalizzata del danno non patrimoniale subito.

(237) Cfr. Cass. civ., sez. un., 5 luglio 2017, n. 16601.

## Parte VIII L'EDUCAZIONE DIGITALE

### 1. La formazione in ambito digitale

#### 1.1 I minori

In Italia, circa un bambino su 3, tra i 6 e i 10 anni, usa lo *smartphone* tutti i giorni. Si tratta di una tendenza in aumento negli ultimi anni.

Il 62,3% dei preadolescenti (11-13 anni) ha almeno un *account social* nonostante la legge (il GDPR) richieda un'età minima di 14 anni (13 anni con l'autorizzazione dei genitori) per fornire il consenso al trattamento dei propri dati *on line* necessari ad aprire un *account*.

Inoltre, i sempre più frequenti episodi di cronaca, che coinvolgono adolescenti e giovani in casi di cyberbullismo, *hate speech*, condivisione di immagini intime senza consenso e altre forme di violenza, rendono ancora più evidente la necessità di promuovere un accesso pieno, competente e sicuro alla rete.

Promuovere una cultura digitale consapevole significa investire nel futuro delle nuove generazioni, affinché possano vivere il *web* come uno spazio di crescita, condivisione e rispetto reciproco. Per realizzare questo obiettivo è fondamentale dare ai più giovani gli strumenti necessari per potenziare le competenze digitali e relazionali: competenze informatiche di base, ma anche la capacità di costruirsi un'identità digitale e conoscenze che permettano di navigare con consapevolezza e spirito critico<sup>(238)</sup>.

#### 2. I percorsi di alfabetizzazione digitale

La vera prevenzione non passa solo dalle leggi ma dalla cultura. Serve promuovere un'educazione digitale che unisca competenze tecniche e consapevolezza etica, capace di far comprendere cosa sia una fonte, come riconoscere una manipolazione e quale impatto possono avere le proprie parole o immagini in rete.

Non possiamo delegare alla tecnologia il compito di risolvere problemi che sono, prima di tutto, umani e sociali. Solo un cittadino informato e consapevole può difendere la propria libertà e quella degli altri. Soprattutto in un momento storico in cui l'intelligenza artificiale è già in grado di creare messaggi mirati, sia testuali che audio o video, personalizzati in base al profilo d'utenza che emerge dalla frequentazione delle piattaforme social.

Occorre offrire percorsi di alfabetizzazione digitale trasversali a tutta la popolazione, per garantire una cittadinanza digitale consapevole e responsabile.

#### 3. La « *media education* »

La *Media Education* (ME) è un'attività educativa e didattica finalizzata a sviluppare nei giovani una comprensione critica circa la

(238) <https://www.savethechildren.it/blog-notizie/educazione-digitale-e-la-guida-con-consigli-genitori-e-adulti>.

natura e le categorie dei *media*, le tecniche da loro impiegate per costruire messaggi e produrre senso, i generi e i linguaggi specifici.

La ME indica: l'educazione «con» i *media*, considerati come strumenti da utilizzare nei processi educativi generali; l'educazione «ai» *media*, che fa riferimento alla comprensione critica dei *media*, intesi non solo come strumenti, ma come linguaggio e cultura; educazione «per» i *media*, livello rivolto alla formazione dei professionisti. Scopo dell'educazione ai *media* è offrire alle nuove generazioni le chiavi per la comprensione dei *media* e promuovere una loro migliore qualità<sup>(239)</sup>.

Per *Gianna Maria Cappello*, presidente dell'Associazione Italiana per l'Educazione ai *Media* e alla Comunicazione (MED)<sup>(240)</sup>, fare *media education* significa aiutare i nostri giovani, i nostri ragazzi a sviluppare consapevolezza critica dinanzi a ciò che ascoltano. Significa, per esempio, insegnare loro a chiedersi perché questo contenuto mi fa ridere, perché questa scena mi sembra normale e perché questo contenuto è diventato virale. Allo stesso tempo significa anche dare strumenti per riconoscere e dire che questo non è amore, questo non è normale, questo non mi fa stare bene. Come tutta l'educazione, anche la *media education* è un investimento a medio-lungo termine sui legami, sulle emozioni, sulla capacità di leggere criticamente il mondo.

Lavorare sulla *media education* – come spiegato da *Maria Ranieri*, vicepresidente dell'Associazione Italiana per l'Educazione ai *Media* e alla Comunicazione (MED)<sup>(241)</sup> – significa maturare competenze critiche educando a comprendere il modo in cui i *media* influenzano le nostre percezioni, emozioni e relazioni. Significa promuovere competenze di carattere emotivo relazionali. Questo aspetto, più psicologico, si sta affermando sempre di più come risposta alle nuove forme di violenza che stanno prendendo il sopravvento in rete. L'obiettivo è promuovere il rispetto, l'empatia, la capacità di gestire le emozioni, i conflitti e far capire i confini tra contesti *on line* e contesti *off line*.

Si deve lavorare sull'*empowerment* digitale delle nuove generazioni fornendo a ragazzi e giovani donne strumenti per riconoscere, segnalare e contrastare la violenza digitale rompendo il silenzio e superando il senso di colpa. La *media education* sviluppa, per sintetizzare, competenze che riguardano sia la comprensione dei messaggi sia la dimensione relazionale, emotiva ed etica dell'uso dei *media*.

(239) <https://www.medmediaeducation.it/cosa-e-la-media-education/>.

(240) Audizione del 4 dicembre 2025.

(241) Audizione del 4 dicembre 2025.

## Parte IX LE CONCLUSIONI E GLI OBIETTIVI

### 1. Le conclusioni

Un'attenta analisi della legislazione vigente ha consentito di evidenziare che il nostro Paese dispone di un valido impianto normativo, recentemente potenziato dalla legge n. 132 del 2025, recante « *Disposizioni e deleghe al Governo in materia di intelligenza artificiale* » che, per contrastare il fenomeno del *deepfake*, ha introdotto il delitto di « *Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale* ».

L'attività conoscitiva posta in essere dalla Commissione, tuttavia, ha consentito di far emergere alcune problematiche.

In primo luogo, il contrasto alla violenza digitale non può più prescindere da un coinvolgimento strutturale e proattivo dei gestori delle piattaforme.

Il passaggio da un regime di mera passività ricettiva a un sistema di obblighi di diligenza qualificata segna il definitivo superamento del dogma della neutralità tecnologica, in favore di una responsabilità sociale d'impresa organicamente applicata all'ecosistema cibernetico. Tale mutamento di paradigma impone l'adozione di protocolli di autenticazione volti all'acquisizione dell'identità digitale certificata, assicurando quella correlazione univoca tra l'utenza virtuale e il soggetto fisico che costituisce il presupposto ineludibile della responsabilità individuale.

A questa necessaria trasparenza deve affiancarsi un presidio di monitoraggio e tutela tempestivo, coordinato da figure di garanzia specificamente deputate al controllo dei contenuti, con un'attenzione prioritaria alle insidie poste dai sistemi di intelligenza artificiale generativa. In tale ottica, i fornitori di servizi sono chiamati a implementare procedure avanzate di riconoscimento e marcatura informatica, garantendo al contempo agli utenti l'accesso a meccanismi di segnalazione semplificati e la facoltà di rimozione immediata dei contenuti, fermo restando l'obbligo del gestore della conservazione dei dati tecnici e dei *log* da mettere a disposizione dell'autorità giudiziaria in presenza di fatti integranti un reato.

La tempestività dell'intervento si configura come l'architrave di questo impianto preventivo e sanzionatorio: i gestori devono assicurare l'oscuramento dei contenuti illeciti, con particolare rigore per quelli a carattere intimo o diffusi in assenza di consenso, entro termini perentori che riducano al minimo la permanenza del danno in rete. Tale obbligo di rimozione deve essere necessariamente integrato dal dovere di inibire la ripubblicazione dei medesimi materiali e dalla conservazione dei dati tecnici e dei *log* per un periodo congruo, al fine di consentire una proficua collaborazione con l'autorità giudiziaria e con l'autorità di vigilanza.

Le evidenze emerse dall'inchiesta delineano, inoltre, la necessità di un intervento normativo che coniughi la celerità della tutela individuale con l'imprescindibile esigenza di conservazione dei mezzi di prova. Si suggerisce, pertanto, di garantire a ogni utente la facoltà di procedere alla rimozione immediata e gratuita o alla modifica dei contenuti e dei

commenti lesivi dallo stesso immessi, compresi quelli generati mediante sistemi di intelligenza artificiale, assicurando al contempo che il gestore della piattaforma mantenga traccia indelebile del contenuto originario. Tale obbligo di conservazione dei dati tecnici e dei *log* di pubblicazione, da estendersi per un congruo periodo da definire, deve indicare con precisione i tempi di permanenza del contenuto sul sito, al fine di consentire una corretta valutazione del danno agevolando la collaborazione con l'autorità giudiziaria per l'eventuale individuazione di profili di illiceità.

L'efficacia di una strategia di contrasto alla violenza digitale risiede nella creazione di un sistema integrato di tutele, all'interno del quale, l'attribuzione di poteri di vigilanza e controllo al Garante per la protezione dei dati personali svolge una funzione di garanzia essenziale e complementare. In un contesto in cui la lesione della dignità umana passa inevitabilmente attraverso l'uso illecito dei dati e delle identità virtuali, l'intervento dell'Autorità si affianca agli altri presidi di legalità, offrendo una via di tutela amministrativa rapida ed efficace a protezione dei diritti fondamentali dell'individuo. L'esercizio di tali potestà non si sostituisce alle competenze dell'autorità giudiziaria ma le integra attraverso un'attività di monitoraggio tecnico sulle modalità di trattamento dei dati da parte dei gestori delle piattaforme. La facoltà del Garante di imporre prescrizioni e di sollecitare la rimozione di contenuti lesivi rappresenta una risposta sussidiaria necessaria, volta a mitigare l'asimmetria di potere tra i grandi attori tecnologici e gli utenti, specialmente nei casi in cui l'inerzia dei *provider* richieda un intervento autoritativo esterno.

In tale prospettiva, l'Autorità agisce come un punto di riferimento fondamentale per la gestione di istanze e reclami che richiedano una protezione specifica del dato personale, assicurando che la difesa contro le patologie del *web* non sia affidata esclusivamente alla discrezionalità dei soggetti privati o ai tempi della giustizia ordinaria, ma benefici di un controllo pubblico specializzato e tempestivo.

Appare indifferibile, inoltre, l'adozione di un paradigma regolatorio che trascenda la mera enunciazione di principi, per approdare a un sistema di tutele presidiato dall'Autorità per le garanzie nelle comunicazioni. Si suggerisce, pertanto, che l'AGCOM sia stabilmente investita di una funzione di coordinamento apicale, agendo come perno di un apparato sanzionatorio caratterizzato da una stringente incisività e dalla capacità di intervenire tempestivamente sulle dinamiche di prevaricazione virtuale. Risulta prioritario che l'Autorità non si limiti a una vigilanza passiva, ma definisca con precisione i protocolli tecnici e i processi procedurali cui i gestori delle piattaforme devono uniformarsi, elevando gli standard di responsabilità e garantendo un monitoraggio rigoroso sulla loro implementazione.

Nell'ottica di una cooperazione istituzionale rafforzata, si propone che l'Autorità attivi procedure di contestazione formale ogniqualvolta emergano violazioni sia d'ufficio sia su impulso del Garante per la protezione dei dati personali o di altri soggetti qualificati.

È auspicabile che tale meccanismo di reazione sia sorretto da poteri coercitivi di natura eccezionale: qualora la diffida ad adempiere entro i termini perentori rimanga inevasa, l'AGCOM dovrebbe disporre del potere di ordinare l'oscuramento della piattaforma telematica o la

sospensione del servizio, fino alla completa rimozione delle criticità. Tale misura interdittiva, affiancata da sanzioni pecuniarie di entità tale da fungere da effettivo deterrente, appare l'unico strumento idoneo a contrastare l'inerzia dei fornitori di servizi digitali dinanzi alla lesione dei diritti fondamentali.

Le risultanze dell'inchiesta parlamentare evidenziano come l'efficacia dell'apparato repressivo e preventivo sia indissolubilmente legata a un sistematico e improrogabile investimento nel capitale umano delle forze di polizia. Si ravvisa la necessità di promuovere programmi di formazione specialistica e aggiornamento permanente per gli operatori della Polizia postale e delle altre Forze dell'ordine, mirati all'acquisizione di competenze tecniche avanzate in materia di intelligenza artificiale generativa. Tale percorso formativo deve consentire agli investigatori di comprendere i meccanismi sottostanti alla creazione, alla manipolazione e alla propagazione dei contenuti sintetici, affinando le capacità di analisi forense necessarie per distinguere i manufatti digitali autentici dalle sofisticate alterazioni algoritmiche. Solo attraverso una classe di operatori dotata di strumenti conoscitivi all'altezza delle sfide tecnologiche contemporanee sarà possibile trasformare i poteri sanzionatori e di oscuramento in azioni concrete e tempestive, garantendo che la risposta dello Stato non risulti mai tardiva o inadeguata rispetto alla velocità della rete.

Il Libro bianco per la formazione degli operatori che entrano in contatto con le donne vittime di violenza curato dal Comitato Tecnico Scientifico dell'Osservatorio sul fenomeno della violenza nei confronti delle donne e sulla violenza domestica, istituito presso il Dipartimento per le pari opportunità della Presidenza del Consiglio dei Ministri, ha dedicato un intero capitolo sulla violenza informatica, a conferma dell'elevata attenzione sul tema da parte di tutti gli attori istituzionali a vario titolo competenti in materia.

Quanto mai opportuna, poi, è la realizzazione di un testo unico delle misure di prevenzione e repressione dei reati digitali. Il testo unico è una raccolta di atti normativi inerenti a una particolare materia con l'obiettivo di rendere maggiormente conoscibile un determinato settore del diritto mediante, per l'appunto, una raccolta sistematica della legislazione vigente relativamente alla medesima tematica. Il ricorso a tale strumento si inserisce all'interno di un percorso di semplificazione dell'apparato burocratico che, inizialmente incentratosi sulla semplificazione amministrativa e sullo snellimento dei procedimenti amministrativi mediante la delegificazione delle norme primarie, si è con il tempo orientato verso obiettivi di riassetto del diritto positivo. Alla luce dell'insieme delle disposizioni già introdotte negli ultimi anni in materia di crimini digitali, la predisposizione di un testo unico di carattere compilativo risponde a un'esigenza di organicità e di effettività dell'ordinamento giuridico, al fine di consentire che le disposizioni vigenti possano trovare una sede comune utile sia per le vittime, per rafforzare la consapevolezza del valore della loro scelta di denuncia e di autodeterminazione, sia per gli addetti ai lavori chiamati ad assicurare la piena tutela della persona offesa, grazie a un quadro più efficace nel garantire reale conoscibilità e quindi effettività delle norme.

Gli esiti della presente indagine, infine, hanno posto in risalto come la risposta repressiva e sanzionatoria, per quanto necessaria, non possa considerarsi esaustiva qualora non venga affiancata da una capillare e strutturale azione di prevenzione culturale. Tale strategia educativa non deve limitarsi alla mera trasmissione di competenze tecniche ma deve mirare alla formazione di una coscienza critica che renda i giovani utenti consapevoli delle implicazioni etiche e giuridiche connesse all'uso delle tecnologie emergenti, con particolare riferimento alla protezione della dignità personale e al rispetto della sfera intima altrui.

## 2. Gli obiettivi

La Commissione parlamentare di inchiesta sul femminicidio, nonché su ogni forma di violenza di genere, istituita con legge 9 febbraio 2023, n. 12, pubblicata nella Gazzetta Ufficiale n. 41 del 17 febbraio 2023, annovera tra i propri compiti quello di «... *proporre soluzioni di carattere legislativo e amministrativo al fine di realizzare la più adeguata prevenzione e il più efficace contrasto del femminicidio e, più in generale, di ogni forma di violenza maschile contro le donne, nonché di tutelare le vittime delle violenze e gli eventuali minori coinvolti* » (articolo 2, comma 1, lettera *m*) della citata legge).

La presente Relazione intende recare gli elementi di proposta utili per la realizzazione degli obiettivi che seguono.

**PUNTO 1****CONTRASTO ALL'ANONIMATO ON LINE: IDENTIFICAZIONE DELL'UTENTE**

Intervenire sull'anonimato *on line* valutando l'adozione di protocolli di identificazione certa per l'accesso e la pubblicazione di contenuti sulle piattaforme digitali, attraverso l'implementazione di sistemi di autenticazione, legati all'identità digitale certificata, che, in caso di violazioni, siano in grado di garantire una correlazione univoca tra l'utenza virtuale e il soggetto fisico, assicurando al contempo il rispetto delle garanzie di tutela della *privacy* e dei dati personali approntate dal quadro normativo interno e unionale. Semplificare le procedure di comunicazione dei dati identificativi all'autorità giudiziaria con imposizione ai *provider* (fornitori di servizi) di obblighi di cooperazione rafforzata – nei termini di conservazione e tempestiva ostensibilità dei dati identificativi – in presenza di richieste della autorità giudiziaria.

**PUNTO 2****OBBLIGO DEI GESTORI DELLE PIATTAFORME DI MONITORAGGIO, INTERVENTO TEMPESTIVO E CONSERVAZIONE DEI DATI**

Introdurre, in linea con la normativa comunitaria, un obbligo di monitoraggio e intervento tempestivo da parte di figure di garanzia specificamente deputate al controllo dei contenuti, implementando le procedure avanzate di riconoscimento e marcatura informatica, garantendo al contempo agli utenti l'accesso a meccanismi di segnalazione semplificati e la facoltà di rimozione immediata dei contenuti (c.d. diritto di ripensamento). Prevedere meccanismi per ottenere l'immediato oscuramento dei contenuti illeciti, con particolare riferimento a quelli a carattere sessualmente esplicito, intimo o comunque incidenti sulla riservatezza della persona, entro termini stringenti così da ridurre al minimo la permanenza in rete e la diffusività « virale » con inibizione della ripubblicazione dei medesimi contenuti. Obbligare il gestore alla conservazione dei dati tecnici e dei *log* per un periodo congruo così da poter essere messi a disposizione delle autorità di vigilanza o dell'autorità giudiziaria.

**PUNTO 3****COMUNICAZIONE DA PARTE DEI GESTORI DELLE PIATTAFORME DELLE *POLICY* E DELLE MODALITÀ DI SEGNALAZIONE**

Favorire, da parte dei gestori e in linea con la normativa comunitaria, la comunicazione delle *policy* e, nel caso dei *social*, degli standard della *community* con modalità chiare e di immediata comprensione, con obbligo di aggiornarli in base all'evoluzione della normativa nazionale e ai *feedback* ricevuti dagli utenti e dagli esperti in materia di tecnologia, sicurezza pubblica e diritti umani. Predisposizione e, se già presenti, semplificazione dei meccanismi di segnalazione e sistemi di reclamo con risposta tempestiva e non stereotipata.

**PUNTO 4****ESTENSIONE A TUTTE LE PIATTAFORME DELL'OBBLIGO DELLA REGISTRAZIONE DEL CODICE « *HASH* »**

Estensione a tutte le piattaforme della registrazione del codice *hash* così da evitare che qualcuno possa caricare il contenuto a fondo

sessuale, acquisito senza il consenso della persona ritratta o filmata, su altre piattaforme.

#### **PUNTO 5**

##### **« DASPO » DIGITALE**

Previsione, da parte delle piattaforme *social*, della sospensione degli utenti che diffondono odio, *deepfake*, *deepnude*, contenuti violenti o lesivi della dignità di terzi, prevedendo un blocco definitivo in caso di accertamento, da parte della autorità giudiziaria, di responsabilità in relazione alla commissione dei c.d. reati digitali.

#### **PUNTO 6**

##### **ESTENSIONE DEL MECCANISMO DI SEGNALAZIONE AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

Estendere la possibilità della segnalazione al Garante per la protezione dei dati personali, prevista dall'articolo 144-*bis* del decreto legislativo n. 196 del 2003 (segnalazione del pericolo di diffusione di immagini o video dal contenuto sessualmente esplicito), anche da parte di chiunque abbia fondato motivo di ritenere che immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a trarre in inganno sulla loro genuinità, possono essere oggetto di cessione, pubblicazione o diffusione attraverso piattaforme digitali senza il suo consenso, affinché il Garante possa intervenire entro le 48 ore successive.

#### **PUNTO 7**

##### **MAGGIORI POTERI DI « ENFORCEMENT » DELL'AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI (AGCOM)**

Attribuire all'AGCOM poteri di *enforcement* (quelli necessari a garantire il rispetto dei regolamenti, come avviare indagini, ordinare la cessazione di violazioni, imporre sanzioni, ecc.) sulle grandi piattaforme e sui prestatori di servizi che non sono stabiliti in Italia anche per quei casi, oltre quelli di violazione del DSA (Regolamento 2022/2065/UE), capaci di causare danni gravi. Istituzione di un punto di contatto unico per il contrasto della violenza digitale di genere che – operando in raccordo con la Polizia postale, le competenti procure della Repubblica, il Garante per la protezione dei dati personali e il Dipartimento per le pari opportunità della Presidenza del Consiglio dei ministri – coordini le segnalazioni prioritarie verso i prestatori di servizi di *hosting* e le piattaforme con il riconoscimento della qualifica di segnalatore attendibile a soggetti qualificati in materia di violenza di genere ai sensi dell'articolo 22 del DSA.

#### **PUNTO 8**

##### **ACCELERAZIONE DELLE PROCEDURE PER IL RILASCIO DELLA QUALIFICA DI SEGNALATORE ATTENDIBILE**

Definire procedure accelerate per il rilascio dello status di « segnalatore attendibile » (*trusted flagger*) a soggetti qualificati ai sensi del *Digital services act* (Regolamento 2022/2065/UE).

**PUNTO 9****POTENZIAMENTO DELLA SICUREZZA DEI MINORI**

Promuovere la sicurezza dei minori tramite l'adozione di misure e protocolli che rendano i loro profili meno raggiungibili da *account* esterni non certificati così da ridurre i crimini digitali ai loro danni.

**PUNTO 10****POTENZIAMENTO DELLE COMPETENZE TECNICO-INVESTIGATIVE NEL CONTRASTO ALLA VIOLENZA DIGITALE**

Proseguire nella promozione di programmi di formazione specialistica e aggiornamento permanente per gli operatori della Polizia postale e delle altre Forze dell'ordine, mirati all'acquisizione di competenze tecniche avanzate in materia di intelligenza artificiale generativa. Obbligo di formazione specifica anche ai magistrati – giudicanti e requirenti, che tabellarmente sono chiamati a trattare i c.d. crimini digitali – e agli avvocati civilisti e penalisti.

**PUNTO 11****POTENZIAMENTO DEL TRATTAMENTO SANZIONATORIO PER LA C.D. *SEXTORTION***

Introdurre la fattispecie autonoma di reato o una specifica circostanza aggravante per sanzionare la c.d. *sextortion* in considerazione della rilevante offensività di tale condotta.

**PUNTO 12****INTRODUZIONE DEL REATO DI DIFFUSIONE ILLECITA DI CONTENUTI SESSUALMENTE ESPlicitI GENERATI O ALTERATI CON SISTEMI DI INTELLIGENZA ARTIFICIALE**

Introdurre una fattispecie di reato che preveda che, salvo che il fatto costituisca più grave reato, chiunque crea, cede, pubblica o altrimenti diffonde contenuti sessualmente espliciti generati o alterati con sistemi di intelligenza artificiale riferibili a una persona identificata o identificabile, senza il suo consenso, sia punito con la reclusione da uno a cinque anni e con la multa da euro 10.000 a euro 50.000, con aggravamento della pena se i fatti sono commessi in danno di minori o da persona che è o è stata legata da relazione affettiva con la persona offesa ovvero se i fatti sono commessi a fini di lucro o con minaccia o violenza.

**PUNTO 13****PRESCRIZIONE DEL DIVIETO DI ACCESSO A INTERNET PER I SOTTOPOSTI AGLI ARRESTI DOMICILIARI PER REATI DIGITALI**

Modificare l'articolo 284 del codice di procedura penale con l'introduzione della prescrizione obbligatoria del divieto della facoltà dell'imputato di accedere ad internet nel caso di sottoposizione alla misura cautelare degli arresti domiciliari per reati digitali.

**PUNTO 14****PATROCINIO A SPESE DELLO STATO PER I « GENDER-BASED DIGITAL CRIMES »**

Estendere il beneficio del patrocinio a spese dello Stato, a prescindere dal reddito della persona offesa, anche per i reati di *revenge porn* (articolo 612-ter del codice penale) e diffusione di immagini create dalla intelligenza artificiale (articolo 612-quater del codice penale) attraverso la modifica del comma 4-ter dell'art. 76 del decreto del Presidente della Repubblica 30 maggio 2002, n. 115, che, allo stato attuale, prevede che « *la persona offesa dai reati di cui agli articoli 572, 575, aggravato ai sensi dell'articolo 577, primo comma, numero 1, nella forma tentata, 577-bis, nella forma tentata, 583-bis, 609-bis, 609-quater, 609-octies e 612-bis, nonché, ove commessi in danno di minori, dai reati di cui agli articoli 600, 600-bis, 600-ter, 600-quinquies, 601, 602, 609-quinquies e 609-undecies del codice penale, può essere ammessa al patrocinio anche in deroga ai limiti di reddito previsti dal presente decreto* ».

**PUNTO 15****DEINDICIZZAZIONE**

Prevedere la possibilità per il giudice civile di emettere ordini inibitori e di de-indicizzazione immediati, anche senza contraddittorio, con sanzioni pecuniarie per ogni giorno di ritardo nell'ottemperanza all'ordine di rimozione dei contenuti illeciti *on line*.

**PUNTO 16****RICOGNIZIONE DEGLI ASSETTI NORMATIVI IN MATERIA DI PREVENZIONE E CONTRASTO DELLA VIOLENZA DI GENERE DIGITALE**

Operare un riordino dei « *gender-based digital crimes* » – nativi o agevolati dalla tecnologia – raccogliendoli in un testo unico che preveda sezioni dedicate agli strumenti di tutela assicurati dalle autorità garanti e dalle autorità giudiziarie così da implementare la coerenza e la completezza della regolamentazione in materia e rendere più agevole la conoscenza dell'impianto legislativo predisposto dal nostro ordinamento.

**PUNTO 17****INTERVENTO SUL CODICE DEONTOLOGICO DEI GIORNALISTI PER CONTENERE IL FENOMENO DELLA « SUPERDIFFUSIONE »**

Suggerire all'Ordine dei giornalisti un intervento sul codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica affinché, allorquando venga data la notizia di vicende relative all'illecita diffusione di immagini o video dal contenuto sessualmente esplicito diffuse senza il consenso delle persone ritratte, non venga indicato il nome del gruppo o del sito (ove ancora attivo) evitando così la c.d. « *superdiffusione* » ossia l'involontaria pubblicità da cui consegue un aumento esponenziale delle visualizzazioni a danno

delle persone ritratte che patiscono una ri-vittimizzazione o vittimizzazione secondaria.

#### **PUNTO 18**

#### **POTENZIAMENTO DELLA EDUCAZIONE DIGITALE, DELL'USO CONSAPEVOLE DEI MEDIA E DELLA CULTURA DELLA PARITÀ DI GENERE**

Continuare ad adottare iniziative di competenza volte a potenziare in modo vincolante le politiche di prevenzione sensibilizzando, altresì, le istituzioni scolastiche del sistema nazionale di istruzione affinché, nell'ambito della loro autonomia e in coerenza con le linee guida per l'insegnamento trasversale dell'educazione civica e con le nuove indicazioni nazionali per la scuola dell'infanzia e del primo ciclo di istruzione, promuovano iniziative finalizzate a rafforzare la cultura della parità di genere, del rispetto reciproco, del rifiuto di ogni forma di violenza, anche attraverso l'utilizzo consapevole degli strumenti informatici, coinvolgendo l'intera comunità educante. Promuovere iniziative di informazione e formazione per gli adulti con analoga finalità.

#### **PUNTO 19**

#### **ISTITUZIONE DI UN TAVOLO TECNICO PERMANENTE O OSSERVATORIO CON RACCOLTA DI DATI**

Istituire un tavolo tecnico permanente sui reati digitali e la violenza di genere *on line* nell'ambito dell'Osservatorio sul fenomeno della violenza nei confronti delle donne e sulla violenza domestica, istituito presso il Dipartimento per le pari opportunità della Presidenza del Consiglio dei Ministri, con funzioni di monitoraggio, analisi e proposta normativa, avvalendosi delle competenze presenti in seno all'Osservatorio e, ove necessario, del contributo di professionalità qualificate.

#### **PUNTO 20**

#### **ASSISTENZA LEGALE E PSICOLOGICA E TECNICA**

Promuovere l'estensione dell'accesso alla assistenza legale e psicologica, prevista per le vittime di violenza di genere e domestica, anche a quelle di violenza digitale. Creazione di una piattaforma nazionale a cui le vittime possano accedere in maniera sicura per ricevere assistenza legale, psicologica e tecnica.

