UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE POLITICHE, GIURIDICHE E STUDI INTERNAZIONALI

Corso di laurea *Triennale* in DIRITTO DELL'ECONOMIA

NUOVE FORME DI LESIONE DEI DIRITTI DELLA PERSONA NEL CONTESTO DELLA MANIPOLAZIONE DIGITALE: IL DIRITTO ALL'IMMAGINE E IL FENOMENO DEL *DEEPFAKE*

Relatrice: Prof.ssa MARIASSUNTA PICCINNI

Laureanda: CARLA MARCHESE
matricola N. 2110132

A.A. 2025/2026

Ai miei genitori,
che hanno reso tutto questo possibile.
Grazie per aver creduto in me,
prima ancora che lo facessi io.

Ai miei nonni,
perché casa, senza voi,
mancava un po' di più.

A mia sorella Rosa,
per aver alleviato la mancanza di casa.

.

INDICE

INTRODUZIONE **3**

CAPITOLO I
IL DIRITTO ALL'IMMAGINE NELL'ORDINAMENTO GIURIDICO NAZIONALE E SOVRANAZIONALE: PROFILI STORICI, NORMATIVI E GIURISPRUDENZIALI

1. Genesi ed evoluzione storica del diritto all'immagine **7**

2. L'evoluzione normativa del diritto all'immagine nell'ordinamento italiano: tra Costituzione e legislazione privatistica **10**

2.1 Definizione del diritto all'immagine *13*

2.2 La natura giuridica del diritto all'immagine, tra dimensione personalistica e rilevanza economica *16*

2.2.1 La disciplina del consenso e le ipotesi di diffusione lecita dell'immagine 21

2.2.2 La rilevanza della notorietà quale criterio di legittimazione della diffusione 23

2.3 L'evoluzione giurisprudenziale a partire dagli anni Novanta *26*

3. La tutela sovranazionale del diritto all'immagine: tra sistema europeo e diritto dell'Unione **28**

3.1 L'immagine dell'individuo come dato personale: la disciplina del GDPR e la tutela della persona *32*

3.2 La protezione del diritto all'immagine nella giurisprudenza della Corte di giustizia UE *34*

3.4. La Convenzione Europea dei Diritti dell'Uomo e la giurisprudenza della Corte EDU *36*

4. Nuove configurazioni del diritto all'immagine nell'era digitale: prime considerazioni **38**

CAPITOLO II
PROFILAZIONE E *DEEPFAKE*: DALLA RACCOLTA DEI DATI ALLA MANIPOLAZIONE DELL'IMMAGINE

1. La *privacy* e l'identità personale: il ruolo dei dati nella società contemporanea **41**

1.1 Profilazione e raccolta dei dati *45*

1.2 L'immagine nel mondo digitale: caso emblematico CapCut *48*

2. *Machine learning*: basi teoriche per l'analisi del fenomeno dei *deepfake* **52**

2.1 Deepfake: nozione *55*

2.1.1 Il fenomeno dei *deepnude* 58

2.1.2 Le *fake news* 60

2.3 L'evoluzione dei deepfake e degli strumenti per il riconoscimento delle manipolazioni *61*

CAPITOLO III
RIMEDI NORMATIVI E TUTELE CIVILISTICHE

1. L'approccio europeo ai rischi dell'ecosistema digitale: il *Digital Services Act* e *Artificial Intelligence Act* **65**

2. Il Garante per la protezione dei dati personali **74**

3. Tutele civilistiche: profili introduttivi **78**

3.1 Tutele preventive: l'azione inibitoria e provvedimenti cautelari *82*

3.2 La responsabilità extracontrattuale: l'art. 2043 c.c. *84*
3.2.1 Gli elementi oggettivi dell'illecito 85
3.2.2 Gli elementi soggettivi dell'illecito 87
3.2.3 Il danno risarcibile 88

3.3 Diritto all'oblio: l'art. 17 GDPR *94*

4. La responsabilità delle piattaforme digitali e l'art. 82 GDPR **97**

4.1 La Direttiva (UE) 2024/2853 sulla responsabilità del produttore per danno da prodotto difettoso *103*

4.2 Regimi speciali di responsabilità: la responsabilità per l'esercizio di attività pericolose *105*

CONCLUSIONE **109**

BIBLIOGRAFIA **114**

SITOGRAFIA **120**

RIFERIMENTI GIURISPRUDENZIALI **123**

INTRODUZIONE

Il diritto all'immagine costituisce una delle più significative espressioni dei diritti della personalità e si colloca al centro del dibattito giuridico contemporaneo, a causa delle profonde trasformazioni sociali e tecnologiche che hanno interessato le società odierne. La tutela all'immagine non riguarda esclusivamente la protezione della rappresentazione fisica dell'individuo, ma investe la sua stessa identità, dignità e libertà personale, in quanto l'immagine rappresenta una proiezione immediata della persona nel contesto sociale[1].
In un'epoca caratterizzata dalla diffusione massiva delle tecnologie digitali e dalla crescente capacità di manipolazione visiva, il diritto all'immagine assume una funzione essenziale quale presidio contro nuove e pervasive forme di aggressione.

L'affermazione moderna dei diritti della personalità e in particolare della centralità della persona trova il proprio fondamento storico e teorico nella stagione successiva al secondo conflitto mondiale. Gli orrori della guerra e le sistematiche violazioni della dignità umana perpetrate dai totalitarismi condussero infatti alla necessità di riformulare il rapporto tra individuo e ordinamento, ponendo la persona al centro del sistema giuridico. È in questo contesto che emerge la figura dell'*Homo Dignus*. La dignità umana diviene così il fondamento assiologico delle democrazie costituzionali contemporanee, imponendo agli ordinamenti non solo di riconoscere formalmente i diritti fondamentali, ma di mettere a disposizione strumenti concreti per la loro effettiva protezione[2].

A questo proposito, il primo capitolo del presente elaborato si propone di analizzare il ruolo del diritto all'immagine nell'ordinamento nazionale, in quello dell'UE e nella dimensione sovranazionale, soffermandosi, nello specifico, sul ruolo svolto dalla Convenzione europea dei diritti dell'uomo. Per quanto concerne la dimensione nazionale, la Costituzione italiana recepisce pienamente la centralità della persona attraverso l'art. 2, che riconosce e garantisce i diritti inviolabili dell'uomo. L'individuo diviene così, il fulcro dell'intero sistema

[1] G. BAVETTA, *Immagine (diritto alla)*, in *Enciclopedia del diritto*, vol. XX, Giuffrè, Milano, 1970, pp. 145-146.
[2] G. AZZARITI, *Stefano Rodotà e l'uso costituzionalmente orientato delle nuove tecnologie*, in Costituzionalismo.it, n.2, Editoriale Scientifica, 2022, pp. 1-2.

costituzionale e non più subordinato alle esigenze dello Stato. Tale centralità trova riscontro anche nella tutela del diritto all'immagine, quale manifestazione diretta della personalità individuale. Nel quadro normativo nazionale, il diritto all'immagine trova specifica disciplina nell'art. 10 del Codice civile e negli artt. 96 e 97 della Legge sul diritto d'autore. Tuttavia, tali disposizioni, elaborate in un contesto storico profondamente diverso da quello attuale, hanno richiesto una costante opera evolutiva da parte della giurisprudenza, chiamata ad adattare i principi tradizionali alle nuove forme di lesione derivanti dall'ecosistema digitale.

Sul piano sovranazionale, la tutela del diritto all'immagine si sviluppa su più livelli. Nell'ambito dell'UE, i testi fondamentali di riferimento, analizzati in questo capitolo introduttivo, sono la Carta dei diritti fondamentali dell'Unione europea, la quale riconosce, agli artt. 7 e 8, rispettivamente il diritto al rispetto della vita privata e familiare e il diritto alla protezione dei dati personali, ed il Regolamento (UE) 2016/679 (GDPR), che rafforza significativamente la tutela dei dati personali di un individuo nello spazio digitale.

Nel più ampio spazio europeo di promozione dei diritti fondamentali, è, poi, centrale, la Convenzione europea dei diritti dell'uomo, che, in particolare attraverso l'art. 8, garantisce il diritto al rispetto della vita privata, offrendo protezioni ulteriori e contribuendo all'evoluzione interpretativa del diritto all'immagine quale diritto fondamentale della persona.

L'evoluzione tecnologica pone, d'altro canto, interrogativi sempre più complessi. La società digitale, fondata sulla raccolta, elaborazione e diffusione continua dei dati espone la persona a rischi inediti, rendendo sempre più vulnerabili i diritti della personalità.
Le tecnologie di intelligenza artificiale, in particolare, hanno amplificato in maniera esponenziale tali problematiche. A questo proposito, il secondo capitolo dell'elaborato si pone l'obiettivo di esaminare come, attraverso i più recenti sistemi di *machine learning*, alimentati da processi di profilazione e addestramento su larga scala, sia possibile creare, alterare e diffondere contenuti sintetici estremamente realistici, incidendo concretamente sulla percezione della realtà.

La profilazione rappresenta uno degli strumenti cardine dell'addestramento dei sistemi di intelligenza artificiale, poiché consente di raccogliere enormi quantità di informazioni, comprese immagini, dati biometrici e comportamentali, utilizzati per perfezionare la capacità generativa dei modelli dell'IA, rendendo il confine tra realtà e finzione sempre più labile, poiché tali tecnologie non si limitano a rappresentare la realtà, ma sono in grado di ricostruirla e modificarla. È in questo contesto che si collocano i fenomeni di c.d. *deepfake*, capaci di compromettere gravemente il diritto all'immagine e l'identità personale. Nel capitolo, la disciplina del *deepfake* sarà introdotta sotto il profilo tecnico per analizzarne il funzionamento e le modalità attraverso cui tali sistemi accrescono la propria efficienza mediante processi di addestramento.

Le tecniche di *deepfake* permettono, infatti, la creazione di video, audio o immagini, spesso indistinguibili dai contenuti autentici, che comportano conseguenze negative non solo rispetto alla tutela dei diritti fondamentali delle persone ritratte, ma anche rispetto ai diritti connessi all'informazione. Tali pratiche si inseriscono in un panorama di illeciti sempre più articolato, comprendente i casi di *deepnude* e diffusione di *fake news*, con effetti dirompenti sia sulla sfera personale dell'individuo che rispetto ai più generali interessi della collettività.

Il problema centrale diviene pertanto quello dell'adeguatezza degli strumenti di tutela predisposti dall'ordinamento rispetto a tecnologie che evolvono con rapidità spesso superiore alle possibilità di evoluzione della regolamentazione normativa. È proprio tale profilo che costituirà l'oggetto di analisi del terzo capitolo. Di fatto, la protezione della persona richiede un approccio multilivello che integri tutele civilistiche, protezione dei dati personali, responsabilità penali e interventi regolatori preventivi, al fine di garantire una risposta effettiva e proporzionata alle nuove forme di lesione digitale. A questo proposito, l'ordinamento interviene con strumenti diversi: sanzionando le condotte più gravi in sede penale e apprestando rimedi risarcitori e inibitori in sede civile; il presente elaborato si concentrerà primariamente sulla tutela civilistica, analizzando l'efficacia dei rimedi privatistici di fronte alla manipolazione dell'immagine.

In questo contesto, assumono rilievo le autorità di controllo come il Garante per la protezione dei dati personali, chiamato a vigilare sul corretto trattamento dei dati e a constatare pratiche lesive della persona. Sul piano normativo, verranno analizzati i recenti Regolamenti: il *Digital Services Act* e l'*Artificial Intelligence Act*, che introducono obblighi specifici di trasparenza e responsabilità.

Le moderne applicazioni dell'intelligenza artificiale se, da un lato offrono straordinarie opportunità di progresso, dall'altro espongono l'individuo a rischi sempre più impattanti, rendendo vulnerabili i diritti della personalità. Il pericolo più significativo è insito nella possibilità che non si trovi un controllo giuridico ed etico adeguato, finendo per alterare l'equilibrio tra innovazione e tutela della persona.

L'ordinamento è chiamato, dunque, ad adattare, attraverso l'evoluzione normativa, l'intervento giurisprudenziale e l'azione delle tutele di garanzia, con specifico riferimento all'azione inibitoria, alla responsabilità extracontrattuale, al diritto all'oblio e ai regimi speciali di responsabilità, affinché il progresso tecnologico resti coerente con i principi costituzionali, con il rispetto della dignità umana e con la salvaguardia dei diritti inviolabili dell'uomo.

In questo scenario, il diritto all'immagine si conferma come uno dei principali ambiti di tensione tra sviluppo tecnologico e tutela della dignità umana, imponendo una riflessione critica sull'evoluzione delle categorie tradizionali dei diritti della personalità e sulla loro capacità di adeguarsi alle sfide poste dalla società algoritmica. La ricerca si propone quindi, di verificare se l'attuale quadro normativo sia in grado di offrire una tutela effettiva al diritto all'immagine rispetto alle nuove forme di manipolazione algoritmica.

CAPITOLO I
IL DIRITTO ALL'IMMAGINE NELL'ORDINAMENTO GIURIDICO NAZIONALE E SOVRANAZIONALE: PROFILI STORICI, NORMATIVI E GIURISPRUDENZIALI

1. Genesi ed evoluzione storica del diritto all'immagine

La tutela dell'immagine, prima della sua piena emersione come diritto, trova le proprie radici concettuali nel diritto romano, in particolare nella figura dell'*iniuria*[3]. Tale istituto rappresentava uno strumento giuridico attraverso il quale l'ordinamento romano riconosceva valore alla dimensione interiore e sociale dell'individuo[4]. L'*iniuria* non si limitava a sanzionare le aggressioni fisiche, ma comprendeva anche le offese all'onore, alla reputazione e alla dignità della persona, anticipando, seppur in forma embrionale, la successiva elaborazione dei diritti della personalità. In tale prospettiva, l'interesse alla rappresentazione di sé e alla percezione sociale dell'individuo viene identificata come una situazione giuridicamente rilevante, pur in assenza di una specifica tutela all'immagine in senso moderno[5].

È solamente con lo sviluppo delle tecnologie di riproduzione visiva che emerge con più chiarezza la necessità di una disciplina specifica che tuteli l'immagine personale. L'avvento della fotografia nel XIX secolo segna un punto di svolta perché rende possibile riprodurre e diffondere con facilità e ampia portata l'aspetto esteriore delle persone[6]. È in tale contesto che possiamo citare le riflessioni di Warren e Brandeis:

> *Even gossip apparently harmless, when widely and persistently circulated, is potent for evil. [...] But now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation*[7].

[3] T. DEIBEL, *The Civil Law and the Inner Self: Roman Iniuria and the Transformation of the Private Sphere*, *Journal of Civil Law Studies*, 16, n. 1, 2024, p. 54.
[4] *Ivi*, pp. 55-56.
[5] *Ivi*, p. 54.
[6] S. D. WARREN, L. D. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, vol. 4, n. 5, 1890, p. 195.
[7] *Ivi*, pp. 196-211.

Mettendo in luce il carattere, anche solo potenzialmente lesivo, della diffusione di contenuti che si riferiscono alla persona e di come si abbia bisogno di tutele sempre più ampie, anche quando la diffusione può sembrare apparentemente innocua. È altresì significativo come le evoluzioni dei mezzi di produzione dell'immagine possano rendere tali lesioni possibili anche senza il coinvolgimento dell'interessato stesso[8], anticipando così la necessità di un diritto autonomo a protezione della persona. Lo sviluppo incessante delle tecniche fotografiche ha determinato un significativo ampliamento delle possibilità di diffusione dell'immagine altrui, nello specifico fa sorgere il problema di quali siano i limiti da imporre per tutelare la persona rispetto alle forme di indebita intrusione nella sfera privata. La possibilità di immortalare individui in atteggiamenti che essi non vorrebbero esporre allo sguardo di terzi, evidenzia il rischio di abusi connessi all'uso indiscriminato dello strumento fotografico. La diffusione non autorizzata dell'immagine viola non solo il diritto alla riservatezza, ma anche il diritto all'estimazione sociale e, nei casi più gravi, il diritto all'onore. L'estrema facilità di accesso agli strumenti di riproduzione delle immagini, e quindi la possibilità che tali mezzi siano alla «*portata di tutti*», ha significativamente ampliato il rischio di interferenze nella sfera privata dell'individuo[9].

È proprio nel contesto statunitense che l'opera "*The Right to Privacy*" di Warren e Brandeis, colloca la prima elaborazione teorica del diritto alla *privacy*, rappresentando un punto di svolta fondamentale. Lo scopo era quello di riconosce per la prima volta il diritto dell'individuo di non subire intrusioni nella sfera privata. Viene formulata così l'idea di un autonomo diritto della *privacy*, inteso come diritto di "*essere lasciati soli*". Gli autori stabilivano come il sistema non dovesse garantire tutela soltanto ai beni materiale o patrimoniali, ma anche agli aspetti morali e spirituali della persona. L'idea di fondo era quella di superare i tradizionali schemi giuridici fondati esclusivamente sulla proprietà privata, sostenendo che la tutela della persona doveva estendersi anche alla tutela della vita privata dell'individuo, riguardando più in generale la salvaguardia della

[8] *Ibidem.*
[9] L. FERRARA, *Il diritto sulla propria immagine nel nuovo Codice civile e nella nuova legge sul diritto d'autore*. Edizioni italiane, Roma, 1942, pp. 11-12.

dignità individuale. Si afferma così, che la lesione del diritto alla *privacy* dovesse essere qualificata come illecito civile (*tort*), limitando la propria elaborazione al solo ambito della *private law of torts*, e quindi sulla mera dimensione negativa della questione (tutela da aggressioni esterne), trascurando così gli aspetti positivi (di promozione del diritto)[10].

Nonostante la portata innovativa dell'opera, il riconoscimento della *privacy* come diritto autonomo non avvenne nell'immediato, in quanto la teoria non si estese all'applicazione a livello costituzionale; essa rappresentò, peraltro, il punto di partenza delle successive elaborazioni dottrinali in materia di *privacy*[11].

Sul piano normativo, un passaggio di rilevanza importante rispetto al riconoscimento del diritto fu rappresentato dall'adozione del *Privacy Act* del 1974, volto a disciplinare il trattamento dei dati da parte delle autorità federali: nello specifico si trattava di una regolamentazione dei rapporti tra governo e privati, lasciando però, la disciplina della *privacy* frammentata per quanto riguardava i rapporti tra privati. La *privacy* nasce, dunque, negli Stati Uniti come strumento di tutela del consumatore e non come diritto fondamentale della persona[12].

Nel contesto europeo, il diritto alla *privacy* ha seguito un percorso differente, posizionandosi come diritto fondamentale della persona e non soltanto come mezzo di tutela di un interesse economico. A partire dagli anni Settanta, il vuoto normativo in materia di tutela dei diritti fondamentali venne progressivamente colmato dalla giurisprudenza della Corte europea di Giustizia, richiamando i principi della Convenzione europea dei diritti dell'uomo, riconoscendo la protezione dei diritti umani quale elemento integrante dell'ordinamento comunitario. In tal modo, molto prima dell'introduzione di specifiche disposizioni normative dedicate ai diritti fondamentali e alla *privacy*, l'ordinamento europeo assicurò una tutela concreta della persona attraverso l'elaborazione

[10] L. MIGLIETTI, *Profili storico-comparativi del diritto alla privacy*, Diritti Comparati, 2014, https://www.dirittocomparati.it/profili-storico-comparativi-del-diritto-alla-privacy/.
[11] *Ibidem*.
[12] *Ibidem*.

giurisprudenziale. Con l'avvento della nascita dell'Unione europea, venne sottoscritta la Carta dei diritti fondamentali dell'Unione europea, costituendo uno dei principali riferimenti per comprendere il fondamento del diritto alla *privacy*, spostando l'attenzione dalla dimensione puramente economica, a quella dei diritti dei cittadini. La Carta riconosce non solo il rispetto della vita privata e familiare, ma riconosce in modo autonomo anche il diritto alla protezione dei dati personali, distinguendo il primo diritto citato, come tutela negativa contro interferenze esterne, ed introducendo per il secondo, una tutela dinamica, volta alla disciplina delle modalità di raccolta, utilizzo e circolazione dei dati ed all'attribuzione all'interessato di specifici poteri di controllo[13].

Le problematiche emerse, rispetto al diritto all'immagine, con la diffusione della fotografia assumono oggi una portata ancora più significativa alla luce delle nuove tecnologie di intelligenza artificiale generativa, che contribuiscono a rafforzare le pratiche del c.d. *deepfake*. Se la fotografia aveva reso possibile la riproduzione e la diffusione non autorizzata dell'immagine di una persona, gli sviluppi dell'intelligenza artificiale consentono, infatti, oggi non solo di riprodurre, ma anche di alterare in modo molto sofisticato l'immagine dell'individuo senza il suo coinvolgimento diretto.

2. L'evoluzione normativa del diritto all'immagine nell'ordinamento italiano: tra Costituzione e legislazione privatistica

In Italia, un primo sintomatico riconoscimento normativo della tutela all'immagine si rinviene all'art. 11 del Reggio Decreto-Legge 7 novembre 1925, n. 1950, convertito in Legge 18 marzo 1926, n. 562. Tale disposizione introduceva una tutela esclusiva dell'immagine personale e stabiliva quanto segue:

[13] *Ibidem*.

> *Il ritratto di una persona non può essere pubblicato o messo in commercio senza il consenso espresso o tacito della persona medesima […][14]. La persona che ha dato il consenso può revocarlo, salvo l'obbligo del risarcimento del danno.*

Un aspetto di particolare rilevanza è rappresentato dall'assenza di distinzioni tra individui noti e individui privi di notorietà, poiché «*hanno essi pure diritto al rispetto della loro persona al pari degli uomini più oscuri*»[15]. La normativa sopra citata presenta un elemento essenziale che rende lecita la divulgazione dell'immagine, cioè il consenso dell'interessato, componente confermata successivamente dal Regio Decreto 13 settembre 1934, n. 1602 relativo alle privative industriali e ai marchi di fabbrica e commercio (d'ora innanzi l. marchi). Nello specifico, l'art. 78 dispone testualmente che:

> *I ritratti di persone non possono essere registrati come marchi senza il consenso delle medesime.*

La disciplina del diritto all'immagine nell'ordinamento italiano ha conosciuto una significativa evoluzione a partire dagli anni Quaranta del secolo scorso. In prima istanza bisogna citare la Legge 22 aprile 1941, n. 633 (d'ora innanzi l. dir. aut.), con particolare attenzione agli artt. 96 e 97; tale disciplina verrà ampliata successivamente con l'introduzione dell'art. 10 del Codice civile del 1942, norma che pur non definendo il concetto di immagine in modo esplicito, riconosce una forma di tutela nei casi di violazione della reputazione del soggetto, la cui lesione è suscettibile di tutela civilistica. In seguito, con l'adozione della Costituzione della Repubblica del 1948, il diritto all'immagine acquisisce rilievo fondamentale, collocandosi come diritto della personalità, anche se il suo fondamento non è previsto esplicitamente. Si può, però, evincere una sua tutela dall'art. 2 della Costituzione che riconosce i diritti inviolabili dell'essere umano. Il riconoscimento giuridico del diritto all'immagine rappresenta l'esito di un lungo sviluppo, fondato in larga misura sull'elaborazione giurisprudenziale, che si estende ben oltre la mera applicazione delle norme esistenti, contribuendo a

[14] «*[…] e, dopo la sua morte, del coniuge e dei figli, o, in loro mancanza, dei genitori, e, mancando il coniuge, i figli e i genitori, degli altri ascendenti e discendenti diretti […]*».

[15] L. FERRARA, *Il diritto sulla propria immagine nel nuovo Codice civile e nella nuova legge sul diritto d'autore*. Edizioni Italiane, Roma, 1942, p. 34.

trasformare una tutela generica della personalità in una protezione progressivamente più specifica e autonoma. Oggi questo diritto riveste un ruolo centrale nella salvaguardia della dignità e della reputazione della persona, costituendo uno strumento imprescindibile per la tutela della sfera individuale e sociale dell'individuo, particolarmente rilevante in un contesto contemporaneo sempre più esposto ai rischi e alle sfide imposte dalle tecnologie moderne. È la stessa Corte costituzionale che ha affermato, con più sentenze, che i diritti della personalità non si esauriscono in quelli espressamente nominati nel testo costituzionale, ma comprendono anche situazioni giuridiche che diventano necessari rispetto all'evoluzione sociale e culturale[16].

La Corte costituzionale con sentenza n. 13 del 1994 fornisce un passaggio fondamentale per la qualificazione dell'identità personale, quale diritto inviolabile della persona, riconducendola all'art. 2 della Cost. Sebbene il caso di specie riguardasse la tutela del nome, la Corte ha elaborato un principio di portata generale, definendo l'identità personale come il «*diritto ad essere sé stesso, inteso come rispetto dell'immagine di partecipe alla vita associata*». Secondo tale orientamento, l'identità personale non è una semplice protezione contro l'uso abusivo delle sembianze fisiche, ma un elemento che appartiene al «*patrimonio irretrattabile della persona umana*», che funge da segno distintivo affinché il singolo possa essere «*individuato, conosciuto e stimato nel proprio ambiente sociale*», ampliando di fatto il concetto di identità personale, collocando l'immagine all'interno di un diritto costituzionalmente protetto e di portata più ampia[17]. La stessa Costituzione impone tuttavia un necessario bilanciamento tra i diritti della personalità e altri diritti, come il diritto di cronaca e di informazione, tutelato dall'art. 21, che riconosce a tutti la libertà di manifestare liberamente il proprio pensiero con ogni mezzo di diffusione. Ne deriva che la tutela dell'immagine non può essere considerata in modo assoluto, ma deve essere costantemente ponderata con l'esigenza di garantire la libera circolazione delle informazioni e il diritto della collettività ad essere informata. In tale prospettiva, il

[16] Cfr. Corte Cost., 7 aprile 1988, n. 404, in cui la Corte riconduce il diritto all'abitazione tra i diritti inviolabili di cui all'art. 2 della Cost., pur in assenza di una sua espressa previsione.
[17] Corte Cost., 3 febbraio 1994, n. 13.

sistema costituzionale richiede che l'esercizio della libertà di informazione avvenga nel rispetto della dignità e dell'identità personale dell'individuo, imponendo un equilibrio tra la protezione della sfera individuale e l'interesse pubblico alla conoscenza dei fatti. Proprio in questo spazio di bilanciamento si colloca il ruolo centrale dell'interpretazione giurisprudenziale, chiamata a individuare, caso per caso, il punto di equilibrio tra la salvaguardia dell'immagine della persona e l'esercizio della libertà di informazione.

Un'ulteriore manifestazione della tutela della persona rispetto all'utilizzo della propria immagine, collocabile nell'evoluzione normativa successiva agli anni Quaranta, si rinviene nell'ambito del rapporto di lavoro. In tale contesto, l'art. 4 dello Statuto dei lavoratori disciplina l'installazione e l'impiego di impianti audiovisivi e di altri strumenti, dai quali, si possa derivare anche la raccolta dell'immagine del lavoratore, subordinandone l'utilizzo a specifiche garanzie procedurali e a finalità organizzative, produttive o di sicurezza. La violazione di tali disposizioni è inoltre sanzionata dall'art. 38 del medesimo Statuto, che prevede conseguenze di natura penale, a conferma della rilevanza attribuita dall'ordinamento alla tutela della dignità e della riservatezza del lavoratore.

2.1 Definizione del diritto all'immagine

La legislazione statale, come espresso in precedenza, non fornisce una definizione testuale e univoca del diritto all'immagine. La disciplina è per lo più frammentata: una nozione astratta si può rinvenire dal combinato disposto dell'art. 10 del Codice civile e dagli artt. 96 e 97 della l. dir. aut. Sotto il profilo strettamente terminologico, però, emerge una peculiarità nel confronto tra le fonti. Da un lato, l'art. 10 Codice civile utilizza la perifrasi «*qualora l'immagine di una persona […]*», per circoscrivere l'oggetto della tutela; il testo utilizza, espressamente la locuzione "*immagine*".

La sezione II della l. dir. aut. e i successivi artt. 96-97-98, al contrario, adottano il termine di "*ritratto*":

Art. 96 «*Il ritratto di una persona non può essere esposto […]. Dopo la morte della persona ritrattata […]*»;

Art 97 «*Non occorre il consenso della persona ritrattata […]. 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»;

Art. 98 «*Salvo patto contrario, il ritratto fotografico […]*».

Nonostante la distinzione adottata dal legislatore, la dottrina e la giurisprudenza hanno superato l'incertezza interpretativa, consolidando i due termini come espressioni equivalenti[18]. Ma, se da un lato si sostiene l'esistenza di una correlazione tra i due concetti, dall'altro si contrappone la tesi secondo cui il termine "*immagine*" costituirebbe una nozione puramente teorica, di per sé inidonea a costruire un valore giuridicamente tutelabile, e sarebbe pertanto preferibile riferirsi al più preciso e circoscritto "*diritto sul proprio ritratto*"[19]. In sostanza, per immagine si intende, di regola, la *rappresentazione visiva* delle sembianze della persona, ovvero, la riproduzione grafica delle sue fattezze in qualunque modo realizzata[20]. Da tale impostazione discende che l'oggetto della tutela non può essere individuato nella mera immagine interiormente concepita, bensì, nella sua concreta esteriorizzazione in una forma suscettibile di percezione e diffusione. Solo con la materializzazione dell'immagine, infatti, si configura quel presupposto oggettivo che consente di valutare l'eventuale lesione del diritto all'immagine[21]. Paradossalmente, l'immagine, non si limita a rappresentare l'aspetto fisico dell'individuo, ma costituisce un'espressione chiara della sua personalità. La violazione di questo diritto non comporta modificazioni materiali del corpo, tuttavia le conseguenze, pur essendo intangibili, investono in modo pervasivo la sfera morale del soggetto[22].

Il diritto all'immagine può essere interpretato secondo una duplice prospettiva. In una prima ottica, di carattere positivo, tale diritto si configura quale espressione della libertà individuale, intesa come autodeterminazione della persona nella

[18] A. SCALINI, *Il diritto alla* riservatezza, Giuffrè, Milano, 2002, pp. 28-29.

[19] M. A. URCIUOLI, *Autonomia negoziale e diritto all'immagine*, Edizioni scientifiche italiane, 2000, p. 71.

[20] A. SCALINI, *Il diritto alla* riservatezza, Giuffrè, Milano, 2002*,* p. 29.

[21] M. A. URCIUOLI, *Autonomia negoziale e diritto all'immagine*, Edizioni scientifiche italiane, 2000, p. 72.

[22] A. SCALINI, *Il diritto alla* riservatezza, Giuffrè, Milano, 2002, p. 33; M. A. URCIUOLI, *Autonomia negoziale e diritto all'immagine,* Edizioni scientifiche italiane, 2000, pp. 92-93.

gestione della propria rappresentazione visiva. L'individuo è titolare del potere di decidere se, quando e in quale modalità mostrarsi al pubblico, nonché di scegliere di non esporsi affatto, esercitando una volontà di riservatezza o di isolamento. In una seconda prospettiva, di carattere negativo, il diritto all'immagine si sostanzia nell'obbligo, in capo ai terzi, di astenersi da qualsiasi forma di riproduzione o divulgazione dell'altrui immagine in assenza del consenso dell'interessato. Tale profilo implica il rispetto della volontà individuale e si traduce nel divieto di interferenze non autorizzate nella sfera personale. La divulgazione dell'immagine altrui, è pertanto lecita, soltanto nei casi previsti dall'ordinamento, quali il consenso espresso o tacito dell'interessato, ovvero le ipotesi normativamente tipizzate in cui la diffusione risulti giustificata da esigenze di interesse pubblico, di cronaca o da altre cause di legittimazione previste dalla legge[23].

Elemento essenziale per configurare la sussistenza di una violazione del diritto all'immagine è la cd. *"riconoscibilità"* della persona ritratta. Ai fini della tutela, è necessario l'identificazione dell'individuo[24].

Diversamente, la cd. *"alterazione dell'immagine"* ricade nell'ambito dell'ingiuria, laddove l'intervento sull'effige comporti una caricatura o deformazione della persona raffigurata. In tali casi, i ritocchi o le modifiche sono idonei a determinare un danno alla reputazione e alla dignità del soggetto. Tuttavia, la tutela attraverso l'istituto dell'ingiuria può trovare applicazione anche in assenza di modifiche materiali dell'immagine: è sufficiente, ad esempio, che la mera esposizione o diffusione da parte di terzi sia idonea a recare pregiudizio alla persona raffigurata[25]. Tali problematiche assumono oggi una rilevanza ancora maggiore con la diffusione dei *deepfake*, in questo contesto, la lesione può derivare sia dalla riconoscibilità del soggetto rappresentato, sia dalla manipolazione artificiale della sua immagine.

[23] A. SCALINI, *Il diritto alla* riservatezza, Giuffrè, Milano, 2002, pp. 30-31.
[24] M. A. URCIUOLI, *Autonomia negoziale e diritto all'immagine*, Edizioni scientifiche italiane, 2000, p. 77.
[25] L. FERRARA, *Il diritto sulla propria immagine nel nuovo Codice civile e nella nuova legge sul diritto d'autore,* Edizioni italiane, Roma, 1942, pp. 255-256.

La Corte di Cassazione, con sentenza 5 aprile 1978, n. 1557[26], ha precisato che l'abusività della pubblicazione non ricorre soltanto in assenza di consenso, ma può sussistere anche quando questo sia stato prestato o quando ricorrano le condizioni che escludono in via ordinaria la tutela della riservatezza, qualora le modalità della diffusione risultino lesive dell'onore, della reputazione o del decoro della persona ritratta. Ne deriva che, la lesione del diritto all'immagine può realizzarsi, sia per la mera diffusione non autorizzata, sia per l'uso dell'immagine in forme che, pur formalmente lecite, si traducano in una rappresentazione denigratoria o comunque idonea a compromettere la dignità personale del soggetto. In tale prospettiva, anche l'esercizio del diritto di cronaca, di critica e di manifestazione del pensiero, pur garantito dall'art. 21 della Cost., incontra un limite invalicabile[27]. L'art. 10 c.c., infatti, non subordina la tutela alla sussistenza di un danno ulteriore rispetto alla diffusione non autorizzata. La lesione si configura nel momento in cui l'immagine viene esposta o pubblicata fuori dai casi consentiti dalla legge e senza il necessario consenso dell'avente diritto, anche in assenza di una concreta compromissione dell'onore o della reputazione, essendo sufficiente la diffusione non autorizzata dell'immagine stessa.

2.2 La natura giuridica del diritto all'immagine, tra dimensione personalistica e rilevanza economica

La sfera dei diritti della personalità si connota per una particolare complessità, che rende difficile definirne l'esatta qualificazione giuridica. Questa difficoltà emerge con chiarezza quando si affronta il tema della natura giuridica del diritto all'immagine.

Nel processo di giuridificazione della persona, il rapporto tra diritti della personalità e modello proprietario si sviluppa inizialmente attorno all'interrogativo circa la possibilità di configurare un diritto della persona su sé stessa, il cosiddetto "*ius in se ipsum*". Le prime elaborazioni, influenzate dalle teorie giusnaturalistiche, muovono da una concezione originaria che configurava i

[26] Sull'evoluzione della giurisprudenza, con riguardo all'evoluzione della nozione di danno risarcibile, si tornerà in modo più approfondito nel corso del cap. 3.
[27] Corte Cass., Sez. I Civile, 5 aprile 1978, n. 1557, massima pubblicata su *Avvocato.it,* https://www.avvocato.it/massimario-36717/.

diritti sulla persona secondo un modello proprietario, secondo cui ciascuno avrebbe una sorta di proprietà sulla propria persona, e dunque anche sul proprio corpo e sui "frutti" dello stesso, tra cui la propria immagine. In questa prospettiva, il problema giuridico consiste nell'individuare se, e, fino a che punto, si può disporre della propria libertà. Il paradigma proprietario implica dunque una rappresentazione della persona come soggetto che "ha" il proprio corpo (è proprietario del), considerato potenzialmente come oggetto di disposizione. Tuttavia, il processo di giuridificazione rivela da subito il carattere ambivalente di questa impostazione: se il riconoscimento di un diritto su di sé potrebbe condurre ad ammetterne la disponibilità, l'intervento del diritto tende al contrario a limitarne i poteri dispositivi, ponendo confini alla disponibilità della persona su sé stessa. Con l'evoluzione storica, il dibattito sullo "*ius in se ipsum*" si amplia progressivamente, includendo non solo gli aspetti materiali, ma anche le sue estrinsecazioni immateriali, quali nome, immagini e opere dell'ingegno. L'inclusione di tali attributi nella categoria dei diritti della personalità accentua ulteriormente il modello proprietario, poiché queste proiezioni acquisiscono valore economico. In questo senso, il diritto disciplina l'utilizzo e la circolazione di tali elementi, cercando di assicurare alla persona il controllo sulle proprie estrinsecazioni materiali e immateriali, talvolta ricorrendo espressamente al paradigma della titolarità esclusiva. Emerge quindi, la duplice anima dei diritti della personalità: da una parte, la dimensione patrimoniale, orientata al controllo e allo sfruttamento economico delle proiezioni della persona; dall'altra, la dimensione assiologica e identitaria, volta alla protezione dei valori fondamentali dell'individuo[28].

Parallelamente, si sviluppa un modello diverso della persona e dei diritti fondamentali, di carattere identitario, nel quale la persona è considerata come centro di valori essenziali che il diritto riconosce e protegge. I diritti della personalità non si circoscrivono più alla sola disponibilità della persona su sé stessa, ma si estendono alla tutela di valori essenziali dell'individuo, quali la vita e l'integrità psicofisica, l'onore, la riservatezza e l'identità personale.

[28] S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie tradizionali al trattamento in massa dei dati personali*, Ledizioni, Milano, 2018, pp. 9-14.

L'ordinamento, infatti, pur riconoscendo alla persona margini di autodeterminazione sul proprio corpo, non ammette disponibilità illimitata, poiché essa viene considerata strumentale alla salvaguardia di valori superiori della persona[29]. Un parallelismo analogo, si riscontra sul fronte degli attributi immateriali. Da un lato, l'onore, la riservatezza e l'identità personale, intesi come valori intrinseci alla dignità umana; dall'altro il nome, l'immagine e i dati personali costituiscono elementi suscettibili di sfruttamento economico, ma la loro disciplina si collega sempre più alla protezione di interessi identitari, come il controllo sulle modalità di rappresentazione sociale della persona. La progressiva patrimonializzazione delle estrinsecazioni immateriali della persona non ha eliminato la loro funzione identitaria; al contrario il valore economico convive con la necessità di preservare l'autenticità della rappresentazione dell'individuo all'interno della società. La progressiva estensione della tutela giuridica dall'immagine al nome, fino all'identità personale e alla protezione dei dati, mostra come il diritto si sia progressivamente spostato da una concezione oggettivante della persona verso una visione incentrata sulla protezione dell'identità e della dignità, pur permanendo profili di sfruttamento economico delle estrinsecazioni della persona stessa. Anche la disciplina dei dati personali riflette la tensione tra paradigma proprietario e paradigma identitario: i dati possono costituire risorse economicamente sfruttabili, ma il loro trattamento coinvolge inevitabilmente la sfera più profonda della persona, incidendo sulla costruzione dell'identità individuale[30][31].

Si colloca in questo alveo, l'evoluzione del diritto all'immagine, il cui raggio d'azione si è progressivamente ampliato: dalla mera protezione delle sembianze

---

[29] Cfr. art. 5 c.c.: «*Gli atti di disposizione del proprio corpo sono vietati quando cagionino una diminuzione permanente della integrità fisica, o quando siano altrimenti contrari alla legge (579 c.p.), all'ordine pubblico o al buon costume (32 Cost.)*».

[30] «*Mentre l'identità, la riservatezza, l'onore, la reputazione e il decoro rappresentano ciascuno un valore e un interesse omogeneo, la protezione dei dati è posta al servizio di interessi eterogenei, che, seppure largamente riconducibili alla comune ratio di mantenere il controllo sulle proprie informazioni, rimangono tra loro fortemente differenziati*», in S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie tradizionali al trattamento in massa dei dati personali*, Ledizioni, Milano, 2018, p. 18.

[31] S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie tradizionali al trattamento in massa dei dati personali*, Ledizioni, Milano, 2018, pp. 13-19.

fisiche alla salvaguardia di qualsiasi elemento idoneo ad evocare la figura del soggetto nel contesto sociale: la difesa dell'immagine ha così assunto uno scopo funzionale a quella dell'identità personale[32]. Su tale questione, la dottrina ha espresso nel tempo posizioni eterogenee che riflettono, *in primis*, differenti modi di intendere il rapporto tra immagine e persona. Sotto questo aspetto, sono due i principali indirizzi teorici. Secondo un primo orientamento, il diritto all'immagine costituisce un diritto inerente alla persona, acquisendo carattere assoluto ed esclusivo. Un secondo orientamento, invece, tende ad oggettivizzare l'immagine, sostenendo una divisione rispetto alla persona, identificandola come entità distinta, suscettibile di autonoma considerazione giuridica. L'orientamento prevalente in dottrina aderisce alla prima impostazione. In tale prospettiva l'immagine è un diritto strettamente inerente alla persona, non è qualcosa di separabile dall'individuo, costituendo una proiezione della sua personalità. L'immagine, al pari del nome e dell'identità, rappresenta l'espressione della propria personalità e per questo, merita tutela[33].

Ulteriore questione dibattuta concerne l'autonomia del diritto all'immagine rispetto agli altri diritti della personalità; si è posto il problema di stabilire se il diritto all'immagine si possa qualificare come diritto autonomo e distinto oppure se la sua tutela si realizzi in connessione con altri diritti della personalità. Anche in questo caso, la dottrina formula diverse tesi: una prima collega il diritto all'immagine direttamente al diritto sul proprio corpo, poiché l'immagine costituirebbe una forma indiretta di utilizzazione del corpo stesso. Tale tesi è stata alquanto criticata, essendo che il diritto all'immagine non si limita al mero aspetto fisico, ma coinvolge la sfera morale e sociale dell'individuo. Un'altra tesi è quella che identifica il sorgere della tutela solo nel caso in cui sia leso l'onore. Tesi che non trova fondamento per via dell'art. 10 del Codice civile, che vieta la pubblicazione dell'immagine altrui anche quando non derivi pregiudizio all'onore o alla reputazione: ne consegue che, il diritto all'immagine acquisisce una propria

[32] Ivi, p. 16.
[33] G. BAVETTA, *Immagine (diritto alla)*, in *Enciclopedia del diritto*, vol. XX, Giuffrè, Milano, 1970, pp. 145.

autonomia e non ha un carattere meramente accessorio rispetto ad altri diritti della personalità[34].

La crescente diffusione di pratiche di sfruttamento commerciale dell'effigie dovuta all'evoluzione del contesto sociale ed economico, con riguardo ai soggetti noti, ha imposto, poi, una rilettura della disciplina in chiave non esclusivamente difensiva. Accanto al potere di vietare l'uso non autorizzato si è progressivamente riconosciuta la facoltà di consentire e controllare lo sfruttamento economico della propria immagine, attraverso l'interpretazione dell'art. 96 della l. dir. aut. che pone il consenso quale presupposto generale di liceità della pubblicazione. Le eccezioni previste dall'art. 97 devono essere interpretate in modo rigoroso, evidenziandone la funzione di informazione dell'interesse pubblico, così da evitare indebite compressioni della sfera individuale. Un ulteriore indice della rilevanza patrimoniale dell'immagine si rinviene nell'art. 21 della legge marchi, che vieta la registrazione come marchio del ritratto altrui senza il consenso dell'interessato. Tale previsione non crea un diritto autonomo di sfruttamento economico, ma presuppone chiaramente che i tratti identificativi della persona possano possedere un valore economico meritevole di protezione. Proprio la crescente valorizzazione di questa dimensione patrimoniale ha alimentato un acceso dibattito circa la possibilità di stabilire un diritto autonomo di utilizzazione economica dell'immagine. In tale prospettiva, parte della dottrina ha elaborato la distinzione tra immagine-documento, intesa quale rappresentazione funzionale all'informazione, e immagine-bene, concepita come fonte di utilità economiche. A quest'ultima verrebbe ricondotto un diritto avente ad oggetto, non il presupposto materiale della raffigurazione, bensì il valore economico che da essa può derivare. Tale impostazione ha il merito di evidenziare con chiarezza la dimensione patrimoniale del fenomeno, ma presenta criticità rilevanti. Separare rigidamente l'immagine dal suo valore economico significa infatti rischiare di frammentare l'unità del bene-persona. L'immagine è una proiezione dell'identità individuale, considerarne il valore commerciale come un bene autonomo, liberamente circolante secondo le logiche del mercato, espone al pericolo di trasformare la

[34] *Ivi*, 146.

persona in oggetto. Il riconoscimento del valore patrimoniale dell'immagine è ormai acquisito, ma non può tradursi in una scissione tra persona e valore commerciale. La tutela deve mantenere al centro l'individuo, cercando un equilibrio tra protezione dell'identità e legittimo sfruttamento economico, senza ridurre l'immagine a un semplice bene di mercato [35].

2.2.1 La disciplina del consenso e le ipotesi di diffusione lecita dell'immagine

Nell'ambito della tutela civilistica del diritto all'immagine, la normativa interna delinea un sistema fondato su una regola generale di protezione e su ipotesi derogatorie tipizzate. La disciplina di riferimento è contenuta negli artt. 96 e 97 della l. dir. aut., che regolano le condizioni di liceità della diffusione dell'effige. L'art. 96 stabilisce che:

> *Il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa*.

Il consenso costituisce, dunque, la principale causa di liceità della divulgazione dell'effige. Il consenso può essere espresso oppure tacito.

Il consenso espresso si manifesta mediante una dichiarazione chiara e inequivoca di volontà, resa verbalmente o per iscritto, con cui il soggetto autorizza la riproduzione e la diffusione della propria immagine entro determinati limiti. A tal fine assume rilievo il criterio interpretativo sancito dall'art. 1362 c.c., secondo cui, nell'interpretazione del contratto, occorre indagare la comune intenzione delle parti e valutare il loro comportamento complessivo. L'autorizzazione alla pubblicazione dell'immagine, quando si inserisca in un rapporto negoziale, si perfeziona secondo lo schema generale delineato dall'art. 1326 c.c., che stabilisce che il contratto è concluso nel momento in cui chi ha fatto la proposta ha conoscenza dell'accettazione dell'altra parte. Il consenso tacito, invece, si desume da comportamenti concludenti idonei a rivelare, in modo non equivoco, l'intenzione di consentire la divulgazione[36].

---

[35] M. A. URCIUOLI, *Autonomia negoziale e diritto all'immagine*, Edizioni scientifiche italiane, 2000, pp. 98-115.

[36] A. SCALINI, *Il diritto alla* riservatezza, Giuffrè, Milano, 2002, pp. 47-53.

Accanto alla regola generale del consenso, l'art. 97 della medesima legge prevede alcune ipotesi tipiche in cui la divulgazione dell'effige è lecita anche in assenza di consenso. La norma dispone che:

> *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.*

Tali eccezioni, sono giustificate dall'esigenza di tutelare interessi della collettività, che prevalgono rispetto al controllo esclusivo sulla propria immagine, consentendo la diffusione anche in assenza del consenso dell'interessato[37]. È opportuno sottolineare che, nei casi in cui la diffusione dell'effigie non sia finalizzata a fornire alla collettività un'informazione di rilevanza sociale, la divulgazione dell'immagine senza il consenso dell'interessato deve considerarsi illecita. Tale tutela si estende anche alle persone note, al fine di prevenire qualsiasi sfruttamento economico della loro immagine. In questa prospettiva, il consenso dell'interessato riveste un ruolo centrale e imprescindibile, soprattutto quando la diffusione dell'effigie avviene per finalità lucrative[38].

Alla luce del quadro normativo esaminato, emerge come la disciplina della diffusione dell'immagine sia costruita secondo una logica di equilibrio tra dimensione individuale e dimensione collettiva. Ne deriva un assetto che, pur riconoscendo centralità alla volontà dell'interessato, ammette limitazioni per la salvaguardia di interessi di rilievo generale.

---

[37] *Ivi*, p. 69.

[38] S. PERON, *Il nuovo perimetro di liceità per la pubblicazione di immagini di un atleta senza il suo consenso*, *MediaLaws, Rivista di diritto dei media*, 2023, https://www.medialaws.eu/il-nuovo-perimetro-di-liceita-per-la-pubblicazione-di-immagini-di-un-atleta-senza-il-suo-consenso/.

2.2.2 La rilevanza della notorietà quale criterio di legittimazione della diffusione

Come evidenziato precedentemente, la notorietà rappresenta una delle condizioni di lecita divulgazione dell'effigie di un soggetto, qualora ricorra un interesse pubblico. È opportuno precisare che, nell'ordinamento vigente, non esiste una definizione normativa di notorietà, una nozione è stata progressivamente costruita nell'elaborazione giurisprudenziale. Tale nozione, che ha accompagnato la definizione giurisprudenziale dei mezzi di tutela, ha avuto un impatto fondamentale per la tutela dell'effige dei soggetti noti, soprattutto nella società contemporanea, caratterizzata dalla diffusione immediata e potenzialmente illimitata dei contenuti attraverso le tecnologie digitali. Il tema assume una particolare centralità, in quanto, è necessario un bilanciamento tra libertà di informazione sancito dall'art. 21 Cost. e tutela della dignità personale che trova tutela negli artt. 2 e 3 Cost., non è sempre facile o scontato e si rende pertanto centrale il ruolo della giurisprudenza nell'adattare i criteri tradizionali alle nuove forme di esposizione mediatica e nella ricerca di una adeguata tutela dei cosiddetti soggetti noti, esposti in misura crescente agli effetti invasivi delle nuove tecnologie, che accrescono il rischio di indebite interferenze nella sfera privata del soggetto.

«*Il concetto di notorietà cui la legge si riferisce configura la particolare situazione sociale di quella persona, che per qualsiasi ragione è conosciuta dalla gran parte degli aggregati ad una comunità, situazione che deve essere in concreto e continuamente verificata*»[39]. Ogni soggetto, di fatto, è conosciuto a livello più o meno differente; in questo caso specifico, invece, la conoscenza si estende a livello pubblico, coinvolgendo non solo un circolo ristretto, ma anche soggetti esterni che non hanno mai avuto una conoscenza diretta con il soggetto noto[40].

Inoltre, la notorietà di un individuo non implica autonomamente la libera divulgazione della sua immagine. Al contrario, proprio in ragione della sua

[39] Così già Trib. Milano, 27 febbraio 1969, cit. in A. SCALINI, *Il diritto alla* riservatezza, Giuffrè, Milano, 2002, p. 73.
[40] *Ivi*, p. 72.

rilevanza pubblica, tale soggetto merita una particolare tutela. La notorietà, infatti, può assumere il valore di circostanza aggravante sotto il profilo economico della pubblicazione: è evidente come la diffusione dell'immagine di una persona già conosciuta sia, di per sé, idonea a generale un vantaggio patrimoniale per il divulgatore[41].

Di fondamentale rilievo, per comprendere il ruolo significativo della giurisprudenza, che ha fatto sì, che la normativa si adeguasse alle necessità dell'ordinamento, è la decisione della Pretura di Roma del 18 aprile 1984. In tale vicenda, Lucio Dalla agiva contro una società che, nell'ambito di una campagna pubblicitaria, aveva utilizzato due accessori, divenuti tratti iconici della figura dell'artista. La pubblicità non riproduceva, né il volto, né le fattezze fisiche del cantante, però, l'utilizzazione dei due accessori, nella percezione collettiva, lo collegarono al cantante nell'immediato. La questione dibattuta risiedeva nella tutela prevista dall'art. 10 Codice civile, e se tale tutela si estendesse, oltre la mera riproduzione diretta dell'effige del soggetto noto, anche agli elementi idonei a identificarla. Nel caso concreto, il giudice affermò che nel caso di persona dotata di elevata notorietà, gli elementi che abitualmente si possono associare alla sua persona, possono assumere una funzione identificativa assumendo parte integrante dell'immagine. Il loro utilizzo ai fini commerciali senza consenso, quindi, è tradotto come una violazione del diritto all'immagine ai sensi dell'art. 10 del Codice civile. La decisione dell'ufficio giudiziario suppone che, per le persone note, l'effige non si limita a coincidere alla rappresentazione della fisionomia, ma comprende l'insieme degli elementi che ne costituiscono l'identità mediatica. La decisione ha portato una significativa evoluzione della tutela, segnando così, il superamento della concezione meramente fisica dell'immagine[42].

Un'ulteriore evoluzione si registra nel caso deciso dal Tribunale di Milano il 26 ottobre 1992, relativo all'impiego pubblicitario di una sosia di Monica Vitti. In

[41] S. SAGLIMBENI, *Privacy e tutela dell'immagine della persona: cosa dice la legge*, Agenda Digitale, 2021, https://www.agendadigitale.eu/sicurezza/privacy/privacy-e-tutela-dellimmagine-della-persona-cosa-dice-la-legge/.

[42] C. DEL RE, *Tutela del diritto all'immagine: nozione estensiva del Tribunale di Milano,* nota a sentenza su *Tribunale di Milano*, *21 gennaio 2014,* pubblicata in *Il diritto industriale*, 2015, n. 3, pp. 295-296.

tale vicenda, la somiglianza tra la sosia e l'attrice, accentuata da trucco, pettinatura e accessori, fu ritenuta sufficiente a integrare una violazione sia dell'art. 10 Codice civile sia degli artt. 96 e 97 della l. dir. aut. Il criterio decisivo fu individuato nella prospettiva del pubblico di riferimento, il quale, a una valutazione poco approfondita, avrebbe potuto ritenere che l'attrice avesse prestato il proprio consenso alla campagna pubblicitaria. La tutela venne dunque estesa anche alle ipotesi di imitazione fisionomica indiretta, equiparando l'uso della sosia alla riproduzione illecita del ritratto[43].

Di particolare rilievo, è altresì, la pronuncia della Corte di Cassazione 12 marzo 1997, n. 2223. La controversia riguardava la commercializzazione di prodotti dolciari contrassegnati da un marchio contenente il nome e tratti stilizzati riconducibili a Totò. La Corte ha affermato che anche la stilizzazione grafica di elementi somatici, combinata con il nome del personaggio, può integrare una lesione del diritto all'immagine qualora l'effetto complessivo del segno distintivo evochi chiaramente la persona nota. Ciò che rileva non è la riproduzione fedele delle fattezze, bensì la capacità del segno di appropriarsi della notorietà altrui e di trarne vantaggio economico[44].

Il diritto all'immagine assume così una duplice dimensione, personale e patrimoniale. Da un lato, esso protegge l'identità e la dignità della persona; dall'altro, tutela il valore economico derivante dalla fama, impedendo che terzi possano appropriarsene senza consenso. La giurisprudenza, pertanto, ha progressivamente ampliato l'ambito applicativo dell'art. 10 c.c., includendovi non solo la riproduzione diretta del ritratto, ma anche l'evocazione indiretta, l'uso di elementi iconici distintivi, la stilizzazione grafica e l'impiego di sosia. In tal modo, viene assicurata una protezione effettiva della persona nota contro forme sempre più sofisticate di sfruttamento pubblicitario, e preservato il valore economico della notorietà.

[43] *Ibidem*.
[44] *Ibidem*.

2.3 L'evoluzione giurisprudenziale a partire dagli anni Novanta

Il quadro normativo precedentemente discusso costituisce il fondamento positivo della tutela del diritto all'immagine, si è definito grazie al ruolo della giurisprudenza che si è rilevato centrale, come già sopra accennato, nel definire i contorni applicativi, colmando le lacune e le ambiguità che il legislatore lascia aperte. Alcune delle pronunce che analizzeremo hanno contribuito a costruire una vera e propria elaborazione sistematica del diritto all'effige, capaci di rispondere ad alcune esigenze cui il semplice dato testuale, non sempre esaustivo, di per sé non era in grado di far fronte. Su questa prospettiva, in particolare per quanto concerne il tema del danno risarcibile e la sua evoluzione in ambito giurisprudenziale, si tornerà per un'analisi più approfondita nel cap. 3.

La sentenza della Corte di Cass. del 16 aprile 1991, n. 4031 segna uno dei momenti decisivi nel quadro giurisprudenziale. Il contesto vede Sergio Cerè diffondere un manifesto nel quale appariva, mediante fotomontaggio, l'immagine di Corinne Picolo, senza che quest'ultima avesse mai autorizzato tale uso. Ottenuta dal Pretore di Milano un'ordinanza di inibizione ex art. 700 c.p.c., la Picolo aveva poi adito al Tribunale di Milano chiedendo la declaratoria di illegittimità dell'uso del materiale e la condanna al risarcimento del danno. Il Tribunale aveva accolto la domanda, decisione confermata successivamente anche dalla Corte di Appello di Milano e infine oggetto del ricorso in Cassazione; quest'ultima, ha evidenziato come non fosse stato prestato il beneplacito del soggetto interessato, precisando che il consenso della posa fotografica per la formazione di un ritratto non si traduce in consenso per la successiva divulgazione del ritratto per scopi commerciali. Inoltre, la mera condotta pregressa della persona ritratta non è sinonimo di consenso per la diffusione dell'immagine e questo non esclude l'illiceità dell'uso non autorizzato[45].

Di particolare importanza è la sentenza del 2 maggio 1991, n. 4785 nella causa Mac S.p.a. c. Armani. Su alcune riviste di moda furono state pubblicati degli annunci riguardanti una campagna promozionale del Comitato Italiano Fodere, in cui comparivano ritratti fotografici di Giorgio Armani e in aggiunta una

[45] Corte Cass., Sez. I Civile, 16 aprile 1991, n. 4031, in *Diritto dell'Informazione e dell'Informatica*, 1991, pp. 835–836.

dichiarazione a lui attribuita, entrambi senza il consenso dell'interessato. Il rappresentante legale di Giorgio Armani, S.p.a. Giorgio Armani, cita in giudizio il Comitato e la S.p.a. Mac, agenzia pubblicitaria, chiedendo la declaratoria di illiceità del comportamento e la condanna al risarcimento del danno. Inizialmente, il Tribunale di Milano aveva affermato l'illiceità dell'atto, ma respinto la richiesta risarcitoria; successivamente la Corte di Appello a seguito di impugnazione da parte di Armani, aveva riconosciuto anche il diritto al risarcimento. La Cassazione asserisce che la divulgazione, quando avviene per finalità pubblicitarie, soprattutto in ragione della notorietà, rende la violazione economicamente rilevante per chi sfrutta l'immagine senza consenso, questo si traduce in un divieto dell'uso del ritratto altrui e dell'illiceità dello sfruttamento del ritratto di una persona celebre per scopi pubblicitari che hanno rilevanza commerciale, senza l'esplicitazione del consenso. Solo il soggetto ritratto è titolare esclusivo del diritto e solo lui può decidere come sfruttare commercialmente la propria immagine[46].

Un altro caso ha coinvolto la Fondazione del Teatro dell'Opera rispetto alla pubblicazione non autorizzata dell'immagine di un ex allievo della scuola di danza del Teatro dell'Opera. La Fondazione aveva inserito la fotografia di G.M. nella locandina promozionale di uno spettacolo, quattro anni dopo che questi aveva cessato di essere allievo della scuola, senza chiedere né ottenere il suo consenso. La Corte di Appello di Roma aveva ritenuto lecita la pubblicazione inquadrandola tra le eccezioni di cui all'art. 97 della l. dir. aut., in quanto rispondeva ad esigenze didattiche collegate all'evento pubblico. La Cassazione ha invece escluso tale interpretazione, affermando che le eccezioni al consenso devono essere interpretate restrittivamente, enunciando la netta esclusione dell'eccezione didattica per eventi culturali, precisando che non si trattava di un saggio scolastico, bensì di un comune evento a pagamento, rientrante nell'attività economica ordinaria della Fondazione. Richiamando il precedente principio per la quale ogni soggetto è titolare della propria immagine, spetta a lui se e come sfruttarla economicamente; nel caso di specie, la diffusione non autorizzata

[46] Ivi, pp. 837–842.

consente all'autore dell'illecito di ottenere indebitamente benefici economici che sarebbero spettati al soggetto leso.[47]

3. La tutela sovranazionale del diritto all'immagine: tra sistema europeo e diritto dell'Unione

Nel contesto giuridico contemporaneo, la tutela dell'immagine si inserisce in un quadro di protezione dei diritti della persona che, non si esaurisce solo con la dimensione normativa nazionale, ma si sviluppa anche sul piano sovranazionale. In ambito europeo, il sistema di garanzie si fonda principalmente sulla Convenzione Europea dei Diritti dell'Uomo e il complesso normativo sviluppato dall'Unione Europea. Quest'ultimo, come vedremo, non si limita alla sola Carta dei Diritti Fondamentali, ma comprende un insieme più ampio di strumenti giuridici e atti normativi che, seppur indirettamente, contribuiscono alla tutela dell'immagine della persona, che comprendono il noto Regolamento Generale sulla Protezione dei Dati Personali (d'ora innanzi GDPR). Verranno, inoltre, analizzate diverse pronunce giurisprudenziali che dimostrano come, in assenza di una previsione esplicita del diritto all'immagine, il ruolo attivo della giurisprudenza abbia assunto un carattere essenziale ed abbia contribuito progressivamente a delineare e adattare alle esigenze contemporanee la tutela di tale diritto nell'ambito dell'Unione Europea.

La tutela dell'immagine nel diritto dell'UE, infatti, non è espressamente prevista come diritto autonomo; tuttavia, essa trova una forma di protezione indiretta attraverso alcune norme primarie dell'ordinamento UE. In particolare, è necessario richiamare la Carta di Nizza, comunemente nota come Carta dei diritti fondamentali dell'Unione europea, documento che sancisce e riconosce i diritti inviolabili della persona, incluso il diritto all'immagine. La Carta è entrata in vigore con il Trattato di Lisbona nel 2009 e, ai sensi dell'art. 6 del Trattato sull'Unione europea, possiede «*lo stesso valore giuridico dei trattati*»[48]. Di conseguenza, le disposizioni in essa contenute producono effetti giuridici nei confronti degli Stati membri. Lo scopo della Carta, come emerge chiaramente, è

[47] Corte Cass., Sez. III Civile, 11 maggio 2010, n. 11353, consultabile su La Legge per Tutti, https://sentenze.laleggepertutti.it/sentenza/cassazione-civile-n-11353-del-11-05-2010.
[48] Trattato di Lisbona, art. 6 TUE.

quello di tutelare i diritti fondamentali della persona e garantire le libertà essenziali dell'individuo all'interno dello spazio giuridico europeo. Essa stabilisce una serie di diritti generali che trovano poi concreta integrazione e specificazione nelle legislazioni interne dei singoli Stati membri. A differenza della CEDU, che si inserisce nel sistema del Consiglio d'Europa quale strumento di diritto internazionale, l'ordinamento dell'UE presente un livello di integrazione più avanzato, poiché alcune fonti del diritto dell'Unione, in particolare i regolamenti e, in determinate condizioni, le direttive, sono direttamente applicabili o comunque idonee a produrre effetti diretti negli ordinamenti degli Stati membri.

Nel Capo I, nello specifico all'art. 1, si afferma un principio fondamentale secondo cui:

> *La dignità umana è inviolabile. Essa deve essere rispettata e tutelata*.

In questo contesto assume particolare rilievo anche la tutela dell'integrità della persona: l'art. 3, comma 1, stabilisce infatti che:

> *Ogni individuo ha diritto alla propria integrità fisica e psichica*.

Tali disposizioni costituiscono il fondamento etico della protezione della persona anche sotto il profilo dell'identità e dell'immagine.

Il Capo II, relativo alle libertà, contiene ulteriori disposizioni rilevanti. L'art. 7 riconosce il diritto al rispetto della vita privata e familiare, stabilendo che:

> *Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni*.

A tale previsione si affianca l'art. 8, dedicato alla protezione dei dati personali, secondo cui:

> *Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*.

Inoltre, il comma 2 specifica che:

> *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.*

Accanto a tali diritti, la Carta riconosce, con l'art. 11, la libertà di espressione e di informazione, che spesso entra in rapporto di collisione con altri diritti fondamentali. L'art. 11, comma 1, dispone infatti che:

> *Ogni persona ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera.*

Infine, il Capo VI, dedicato alla giustizia, rafforza la tutela dei diritti fondamentali attraverso garanzie processuali. In particolare, l'art. 47 prevede il diritto a un ricorso effettivo e a un giudice imparziale, stabilendo che:

> *Ogni persona i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice.*

Le norme contenute nella Carta si inseriscono all'interno di un quadro valoriale esplicitato nel suo stesso preambolo, secondo cui:

> *L'Unione si fonda sui valori indivisibili e universali della dignità umana, della libertà, dell'uguaglianza e della solidarietà; essa si basa sui principi della democrazia e dello Stato di diritto. Pone la persona al centro della sua azione istituendo la cittadinanza dell'Unione e creando uno spazio di libertà, sicurezza e giustizia*[49].

In questo contesto, l'interpretazione coordinata di tali diritti consente di individuare un solido quadro di garanzie volto a proteggere la persona anche rispetto all'utilizzo e alla diffusione della propria immagine, richiedendo al contempo un costante bilanciamento con altri diritti fondamentali, tra cui la libertà di espressione e di informazione. Proprio per via dell'assenza di un diritto esplicito dell'effige all'interno dell'ordinamento europeo, nei vari paesi membri si

[49] Dipartimento per le Politiche Europee. *Carta dei diritti fondamentali dell'Unione europea*, 2025, https://www.affarieuropei.gov.it/it/normativa/diritti-fondamentali/carta-dei-diritti-fondamentali-dellue/.

trova una frammentazione di tale diritto che molte volte, in via distinta trova tutela nel diritto della *privacy* o nei diritti della personalità[50].

Come precedentemente esaminato, con riferimento all'ordinamento italiano e, più ampiamente nello spazio europeo, il diritto all'effige o, più in generale, i diritti della personalità, possono, in determinate circostanze, entrare in conflitto con altri diritti riconosciuti dal medesimo ordinamento. La complessità di questo bilanciamento accomuna molti ordinamenti nazionali degli stati europei. In particolare, il cd. "diritto d'autore" si trova frequentemente a collidere con altri diritti della persona, tra cui, nel caso specifico oggetto di analisi, con il diritto all'immagine.

A tal proposito, si richiama, una decisione della *Cour de cassation* francese (*1ère chambre civile*, 20 *mars* 2007, *Bull.* 2007, I, n. 125, *pourvoi n.* 06-10.305)[51]. Nel caso di specie, un noto artista aveva utilizzato alcune fotografie di natura intima per realizzare opere d'arte. La donna ritratta si opponeva alla divulgazione delle opere. Dall'altra parte, il noto artista invocava la tutela della libertà di espressione espressamente prevista all'art. 10 della Convenzione europea dei diritti dell'uomo[52]. La Corte francese ha cercato di trovare un bilanciamento tra i diritti in conflitto, distinguendo tra le diverse immagini utilizzare. Per alcune fotografie, rispetto alle quali risultava prestato il consenso della donna, la divulgazione è stata ritenuta legittima. Diversamente, con riferimento alle opere che rappresentavamo la donna in situazioni di particolare intimità, la corte ha ritenuto prevalente la tutela dell'immagine, affermando che la mancanza di consenso della persona ritratta dovesse prevalere sulla libertà di espressione dell'artista. È,

[50] T. SYNODINOU, *Image Right and Copyright Law in Europe: Divergences and Convergences*, in *Laws*, vol. 3, n. 2, 2014, p.183.
[51] Cour de cassation, 1ère ch. civ., 20 mars 2007, n. 06-10.305, in T. SYNODINOU, *Image Right and Copyright Law in Europe: Divergences and Convergences*, *Laws*, vol. 3, n. 2, 2014, pp. 189-190.
[52] «*Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche […] L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario*».

quindi, proprio la presenza del consenso che definisce quale diritto prevale rispetto ad un altro[53].

3.1 L'immagine dell'individuo come dato personale: la disciplina del GDPR e la tutela della persona

L'immagine di una persona può essere ricondotta alla nozione di dato personale e, in quanto tale, è soggetta alla disciplina relativa al trattamento dei dati personali. Tale qualificazione assume una rilevanza sempre maggiore a seguito delle recenti evoluzioni tecnologiche e delle nuove sfide poste dal fenomeno dei *deepfake*.

Nel contesto dell'ordinamento giuridico nazionale, la materia era originariamente regolata dal D.lgs. n. 196/2003, noto come Codice *Privacy*, successivamente modificato e adeguato dal D.lgs. n. 101/2018 al fine di recepire e armonizzare la normativa interna con quanto previsto dal Regolamento (UE) 2016/679, meglio conosciuto come Regolamento Generale sulla Protezione dei Dati (GDPR)[54]. L'evoluzione normativa, non si circoscrive al solo ordinamento nazionale, ma si inserisce in un percorso più ampio a livello europeo, che trovava il proprio antecedente nella Direttiva 95/46/CE[55], che ha rappresentato il primo intervento organico a livello comunitario in materia di tutela dei dati personali, ponendo le basi dei principi che verranno sviluppati in seguito e in modo più dettagliato nel GDPR.

L'art. 4 lett. b del Codice della *Privacy* forniva come definizione di dato personale:

> *Qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.*

[53] T. SYNODINOU, *Image Right and Copyright Law in Europe: Divergences and Convergences*, *Laws*, vol. 3, n. 2, 2014, pp. 189-190.
[54] 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).
[55] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

L'art. 4 (n.1) del GDPR amplia tale nozione, includendo in modo più esplicito l'immagine della persona quale elemento idoneo a identificarla. L'immagine è qualificabile come dato biometrico nei casi di trattamenti tecnici specifici volti a consentire l'identificazione della persona, come ad esempio, nei sistemi di riconoscimento facciale. In particolare, l'art. 4 del GDPR, tra le definizioni preliminari (n.14), riconduce l'immagine facciale tra i dati biometrici, qualora essa consenta l'identificazione univoca di un individuo, nello specifico l'articolo prevede quale nozione di dati biometrici:

> *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*[56].

Richiamando il considerato n. 32, si percepisce come elemento fondamentale il consenso dell'interessato, la premessa introduttiva segue così:

> *Il consenso dovrebbe essere prestato mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano […] qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto*[57].

È l'art. 13 del GDPR a disciplinare il contenuto delle informazioni che devono essere fornite all'interessato quando i dati personali sono raccolti direttamente presso di lui. La norma impone al titolare del trattamento un obbligo di trasparenza, prevedendo che l'interessato sia informato in modo chiaro e comprensibile circa l'identità del titolare, le finalità e la base giuridica del trattamento, l'eventuale comunicazione dei dati a terzi, il periodo di conservazione e i diritti riconosciuti all'interessato stesso. In questo modo si

---

[56] M. BOGDANOVIC, *Il diritto alla tutela dell'immagine personale. Disciplina, problematiche e modello di liberatoria*, *Altalex*, 2020, https://www.altalex.com/documents/news/2020/10/29/diritto-tutela-immagine-personale.

[57] «*Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso*».

garantisce che la persona sia pienamente consapevole delle modalità con cui i propri dati, inclusa l'immagine, vengano trattati. Accanto a tale disposizione, l'art. 14 disciplina l'ipotesi in cui i dati personali non siano raccolti direttamente dall'interessato, ma provengano da altre fonti. Anche in questo caso il titolare del trattamento è tenuto a fornire all'interessato una serie di informazioni analoghe a quelle previste dal precedente articolo, con l'aggiunta dell'indicazione della fonte da cui i dati sono stati ottenuti e, se ricorre il caso, della circostanza che provengano da fonti accessibili al pubblico. La *ratio* dell'articolo è quella di evitare che il trattamento di dati personali avvenga all'insaputa dell'interessato, garantendo comunque un adeguato livello di trasparenza e permettendo alla persona di esercitare i propri diritti anche quando i dati non siano stati raccolti direttamente presso di essa. Nel complesso, le disposizioni contenute negli artt. 13 e 14 esprimono il principio di trasparenza e di correttezza del trattamento dei dati personali, imponendo al titolare un preciso obbligo informativo che consente all'interessato di conoscere e comprendere le modalità con cui i propri dati vengano utilizzati. Nello specifico, l'individuo deve essere messo nella condizione tale da sapere chi utilizza la sua immagine e le finalità.
Il GDPR assicura una tutela dell'immagine in quanto dato personale, imponendo limiti e condizioni al suo utilizzo, assicurando così un bilanciamento tra protezione dei diritti fondamentali e le esigenze di trattamento dei dati personali. Le più recenti evoluzioni tecnologiche pongono nuove sfide cui si è tentata una risposta anche a livello UE attraverso lo sviluppo di strumenti normativi più specifici, di cui si tratterà nel cap. 3.

3.2 La protezione del diritto all'immagine nella giurisprudenza della Corte di giustizia UE

Al fine di comprendere in modo più dettagliato come trovi concreta tutela il diritto all'immagine, risulta proficuo analizzare la giurisprudenza delle Corte dell'Unione Europea attraverso l'esame di alcune decisioni, alcune delle quali si riferiscono alla normativa precedente al GDPR. È possibile osservare come la normativa dell'Unione Europea venga applicata e interpretata in base alle necessità del caso concreto, contribuendo a delineare i limiti e le condizioni di laicità dell'uso dell'immagine di un individuo.

In via preliminare, appare opportuno richiamare l'orientamento espresso dalla Corte di giustizia dell'Unione Europea nella sentenza 8 dicembre 2022, causa C-460/20, che ha riconosciuto che l'immagine costituisce uno degli attributi fondamentali della personalità dell'individuo, il diritto alla sua tutela di fatto implica il controllo dell'individuo sulla propria rappresentazione e sulla sua diffusione. In questa prospettiva, pur rientrando la pubblicazione di fotografie nell'ambito della libertà di espressione e di informazione, la protezione della vita privata assume un rilievo significativo, in considerazione della capacità delle immagini di veicolare informazione anche intime[58].

Nella sentenza 24 settembre 2019, causa C-136/17, la Corte afferma che, l'attività dei motori di ricerca costituisce un autonomo trattamento di dati personali capace di incidere significativamente sulla rappresentazione pubblica dell'individuo, poiché consente la costruzione di un profilo accessibili globalmente a partire dal nome della persona. Ne deriva che il gestore del motore di ricerca è tenuto a garantire una tutela concreta ed effettiva dei diritti fondamentali, in particolare del diritto al rispetto della vita privata e alla protezione dei dati personale, anche mediante strumenti come la deindicizzazione. La Corte chiarisce che tale tutela è particolarmente incisiva quando i dati trattati riguardano aspetti intimi della persona, imponendo limiti e obblighi stringenti. La protezione non deve essere intravista come tutela assoluta, infatti, nella sentenza si rinvia agli artt. 7, 8 e 11 della Carta dei diritti fondamentali dell'Unione Europea, una tutela al diritto all'immagine deve essere bilanciata con il diritto alla libertà d'espressione e di informazione, specie nei casi che riguardano interessi di carattere pubblico.[59]

La sentenza C-345/17 assume particolare rilievo per l'ambito applicativo della Direttiva 95/46/CE, nonché nell'interpretazione della deroga prevista per le attività giornalistiche con riferimento alla pubblicazione *online* di contenuti audiovisivi, affermando che la registrazione video di persone identificabili, anche se effettuate da un privato e la successiva diffusione su piattaforme digitali

[58] *È illecita la diffusione di foto di un minore senza il consenso di uno dei genitori?, Lexet*, 2024, https://lexet.it/e-illecita-la-diffusione-di-foto-di-un-minore-senza-il-consenso-di-uno-dei-genitori/.
[59] CGUE, 24 settembre 2019, C-136/17.

costituiscono un trattamento ai sensi della Direttiva. L'immagine e la voce di una persona sono qualificate come dati personali, in quanto idonee a consentirne l'identificazione. La protezione dei dati rappresenta un diritto importante nell'ordinamento dell'Unione europea, imponente che i trattamenti dei dati personali avvenga rispettando le garanzie previste dalla normativa; la Corte a questo proposito richiama la necessità di bilanciare la raccolta dei dati con la libertà di espressione, alla luce della deroga prevista per le attività giornalistiche, come espressamente previsto dall'art. 9 della Direttiva[60], che introduce un'interpretazione ampia, ma qualora il trattamento sia finalizzato alla diffusione di informazioni e opinioni di interesse pubblico[61].

Tali principi assumono rilevanza, in modo più ampio, anche nel contesto digitale contemporaneo, caratterizzato dal rapido evolversi di mezzi tecnologici sempre più pervasivi, in cui la diffusione e l'elaborazione di informazioni personali possono incidere in modo significato sulla sfera individuale. L'idea di base, è quella di limitare utilizzi incoerenti dei dati personali, evitando che le informazioni raccolte siano trattare per scopi disgiunti rispetto a quelli originali.

3.4. La Convenzione Europea dei Diritti dell'Uomo e la giurisprudenza della Corte EDU

La Convenzione Europea dei Diritti dell'Uomo (CEDU), adottata nell'ambito del Consiglio d'Europa, rappresenta uno dei principali strumenti internazionali per la tutela dei diritti umani e delle libertà fondamentali. Tutti i 46 Stati membri del Consiglio d'Europa hanno aderito a tale trattamento, impegnandosi a garantire i diritti in esso sanciti. La Convenzione ha inoltre istituito la Corte Europea dei Diritti dell'Uomo, organo giurisdizionale incaricato di assicurare l'effettiva protezione dei diritti presenti nel testo. L'Italia ha ratificato la CEDU con la legge 4 agosto 1955, n. 848. Come evidenziato in precedenza, nell'ordinamento sovranazionale non esiste un esplicito e autonomo diritto all'immagine riconosciuto in modo diretto. Tuttavia, la lacuna normativa non implica una

[60] «*Gli Stati membri prevedono, per il trattamento di dati personali effettuato esclusivamente a scopi giornalistici o di espressione artistica o letteraria, le esenzioni o le deroghe alle disposizioni del presente capo e dei capi IV e VI solo qualora si rivelino necessarie per conciliare il diritto alla vita privata con le norme sulla libertà d'espressione*».
[61] CGUE, 14 febbraio 2019, C-345/17.

mancanza di tutela effettiva, ma tramite un'interpretazione sistematica delle norme, si trova una protezione a tale diritto. In questo contesto, assume ruolo centrale la giurisprudenza della Corte Europea dei Diritti dell'Uomo, che ha sviluppato un approccio dinamico nella salvaguardia del diritto all'immagine. La tutela, anche se non espressamente prevista, viene ricondotta principalmente all'articolo 8 della Convenzione, relativo al diritto al rispetto della vita privata e familiare[62]. Tale diritto, tuttavia, non opera in modo assoluto, ma richiede un constante bilanciamento con altri interessi, già indicati nell'art. 8 e meglio esplicitati in altri diritti riconosciuti dalla stessa Convezione, tra cui, non si può non menzionare, l'articolo 10 che tutela la libertà di espressione[63]. La Corte è chiamata a bilanciare i diversi interessi confliggenti caso per caso, attraverso un'attenta ponderazione dei valori in gioco.

La tutela del diritto all'immagine nell'ambito della Convenzione europea dei diritti dell'uomo è il risultato di una progressiva elaborazione da parte della giurisprudenza della Corte europea dei diritti dell'uomo degli strumenti normativi presenti nell'ordinamento europeo. L'art. 8, citato precedentemente, non include espressamente il diritto all'immagine, la Corte ha fornito un'interpretazione in senso ampio fino ad includere nel medesimo articolo anche gli aspetti legati all'identità personale e alla rappresentazione visiva dell'individuo.

In particolare, la sentenza *Von Hannover* c. Germania segna un punto fermo nella protezione dell'effige contro le intrusioni mediatiche. La Corte affronta il tema

---

[62] «1. *Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. 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 o della morale, o alla protezione dei diritti e delle libertà altrui*».

[63] «*1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, cinematografiche o televisive. 2. L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario*».

della pubblicazione di fotografie riguardanti la principessa Carolina di Monaco in momenti della vita quotidiana. In questo contesto, la Corte chiarisce che, anche i soggetti noti godono della tutela della vita privata e precisa che la pubblicazione di immagini di persone note è lecita solo se contribuisce all'interesse generale e pubblico. In assenza di tal requisito, prevale la tutela dell'individuo, segnando un punto fermo nella protezione dell'effige contro le intrusioni mediatiche[64].

Da citare anche la sentenza Sciacca c. Italia, in cui la Corte si concentra sull'operato delle autorità pubbliche, ritenendo che la diffusione delle fotografie segnaletiche di una persona indagata, da parte di un organo di polizia, costituisca una violazione del diritto sancito dall'art. 8 e, quindi, una violazione al rispetto della vita privata. Si evidenzia come la pubblicazione della fotografia segnaletica della ricorrente abbia costituito un'ingenza nella sua vita privata, non giustificata da interesse pubblico. La sentenza identifica come la tutela dell'immagine, intesa come aspetto del rispetto vita privata, non sia circoscritta ai soli consociati, ma si estenda nei confronti dello Stato[65].

Nella controversia *Couderc* e *Hachette Filipacchi Associés* c. Francia, la Corte specifica come la libertà d'espressione costituisce uno dei fondamenti essenziali di una società democratica, ma precisa che, essa, può prevalere sul diritto all'immagine solo quando sussista un reale interesse pubblico riguardante la diffusione di specifiche informazioni[66].

4. Nuove configurazioni del diritto all'immagine nell'era digitale: prime considerazioni

Il ruolo delle Corti, a livello nazionale e sovranazionale, come abbiamo visto nei precedenti paragrafi, consente il riconoscimento e la tutela di diritti che non sono sempre espressamente previsti a livello normativo, attraverso un'interpretazione estensiva delle stesse norme e permette, attraverso la necessaria attività interpretativa, di bilanciare i contrapposti interessi, adeguando le norme alle necessità del caso specifico. La natura dinamica ed evolutiva della giurisprudenza

[64] CEDU, *Von Hannover c. Germania*, 24 giugno 2004, n. 59320/00.
[65] CEDU, *Sciacca c. Italia*, 11 gennaio 2005, n. 50774/99.
[66] CEDU, *Couderc e Hachette Filipacchi Associés c. Francia*, 10 novembre 2015, n. 40454/07.

permette di dare risposte più adeguate in replica alle continue necessità e trasformazioni della società contemporanea. Questo è emerso in modo significativo anche nell'ambito della giurisprudenza della Corte EDU, la quale ha chiarito l'importanza del diritto all'immagine come componente essenziale della personalità. In particolare, nella sentenza *Reklos* e *Davourlis* c. Grecia ha affermato che:

> *A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers*[67].

Se la disciplina tradizionale era stata elaborata principalmente con riferimento alla fotografia, poi all'avvento della televisione e dei mezzi di comunicazione di massa, il rapido progresso tecnologico, conseguente dapprima alla diffusione di *internet* e dei *social* e, da ultimo, all'avvento dell'intelligenza artificiale generativa, pone oggi, nuove problematiche rispetto alla tutela dell'identità personale e del diritto all'immagine. L'evoluzione tecnologica e la progressiva digitalizzazione delle relazioni sociali impongono al diritto un constante processo di adattamento, soprattutto con riferimento ai diritti della personalità. Il diritto all'immagine e la sua relativa evoluzione, oggi assume una dimensione più complessa. In questo senso, l'immagine, diviene parte integrante di un ecosistema digitale fondato sulla raccolta e la circolazione dei dati personali. La presenza dell'individuo nelle piattaforme digitali contribuisce alla formazione di una vera e propria identità digitale suscettibile di manipolazione artificiale mediante strumenti tecnologici sempre più all'avanguardia. A tale proposito, il fenomeno della profilazione, attraverso il quale l'identità personale tende a trasformarsi in una proiezione digitale costantemente analizzabile, espone il soggetto a nuovi rischi di lesione dei propri diritti.

Tra le tecnologie maggiormente invasive emergono i *deepfake*. Tali strumenti pongono questioni giuridiche di particolare rilevanza, poiché incidono sull'affidabilità della rappresentazione digitale del soggetto, ledendo il diritto alla propria immagine. Il prossimo capitolo sarà dunque dedicato all'analisi del

[67]CEDU, *Reklos e Davourlis c. Grecia*, 15 gennaio 2009, n. 1234/05.

fenomeno de *deepfake* e di come queste tecnologie diventino sempre più sofisticate, riducendo la possibilità di distinguere il reale dal falso, al fine di comprendere le modalità attraverso cui tali tecnologie operano e le ragioni per cui esse costituiscono una delle più significative minacce contemporanee alla tutella dell'immagine e dell'identità digitale della persona.

CAPITOLO II
PROFILAZIONE E *DEEPFAKE*: DALLA RACCOLTA DEI DATI ALLA MANIPOLAZIONE DELL'IMMAGINE

1. La *privacy* e l'identità personale: il ruolo dei dati nella società contemporanea

La *privacy* si definisce tradizionalmente come il «*diritto di essere lasciati soli*»[68], nella società contemporanea questa nozione muta e assume un significato diverso, identificandosi come il diritto di controllare l'uso delle informazioni personali che riguardano l'individuo e che contribuiscono a definire l'identità nella società dell'informazione[6970].

Lo sviluppo delle tecnologie ha trasformato profondamente le modalità di raccolta e utilizzo dei dati, imponendo una nuova prospettiva sul concetto stesso di *privacy*: non si tratta più di difendere la vita privata dalle intrusioni esterne, ma di comprendere chi detiene le informazioni e come queste vengano impiegate[71]. L'enorme quantità di dati raccolti rende centrale la questione del controllo, spostando l'attenzione sulla possibilità di ciascun individuo di gestire i propri dati personali nel concreto, questo perché il possesso delle informazioni implica un aumento del potere, capace di influenzare decisioni e comportamenti; basti pensare alle nuove forme di comunicazione politica sviluppatesi nell'ambiente digitale, il cosiddetto *cyberpopulismo*[72], in cui l'uso strategico dei dati e delle piattaforme, consente di orientare il consenso e di istaurare un rapporto potenzialmente manipolato tra esponenti politici e cittadini. Nel caso di specie, i

[68] Storicamente, la *privacy* si è affermata come un diritto tipico delle classi più agiate, mentre risultava, di fatto, assente nelle condizioni di vita della classe operaia durante la rivoluzione industriale. Le analisi di Engels sulle città inglesi mostrano come il sovraffollamento e la povertà impedissero qualsiasi forma di vita privata. In questo senso, *privacy* e povertà apparivano incompatibili, *«il diritto di essere lasciati soli»* poteva assumere un significato negativo, se inteso come indifferenza verso condizioni dei più deboli, in S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, Bologna, 2021, p. 28.

[69] G. FINOCCHIARO, *Identità personale (diritto alla)*, in *Digesto delle discipline privatistiche*, UTET, Torino, 2010, p. 727.

[70]Alan F. Westin definisce la *privacy* come «*il diritto della persona di controllare l'uso che gli altri fanno delle informazioni che la riguardano*». Cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, Bologna, 2021, pp. 97-98.

[71] *Ivi*, pp. 25-26.

[72] «*Propaganda politica esercitata mediante la rete telematica per evidenziare il coinvolgimento delle masse popolari*» in Enciclopedia Treccani, voce *Cyberpopulismo.*

dati personali tendono ad essere mercificati e utilizzati per attività di profilazione, contribuendo al condizionamento delle scelte degli elettori[73]. In una prospettiva critica, la filosofa Adriana Cavarero sottolinea come il populismo digitale possa mettere in discussione l'idea di una democrazia realmente diretta, poiché gli individui vengono esposti a contenuti selezionati dagli algoritmi che filtrano e orientano l'informazione[74].

Basti pensare al caso "*Cambridge Analytica*" in cui i dati di milioni di utenti *Facebook* sono stati raccolti e utilizzati senza consenso per finalità di profilazione politica, influenzando campagne elettorali, come quella presidenziale di Donald Trump[75].

D'altronde, è irrealistico pensare di arrestare la raccolta dei dati, ormai necessaria per il funzionamento delle organizzazioni moderne, però diventa fondamentale individuare un equilibrio tra la tutela delle libertà individuali e dell'efficienza delle strutture che utilizzano tali informazioni[76]. Nei tempi più recenti, inoltre, la questione non riguarda più soltanto la protezione dei dati in sé, ma anche le modalità con cui essi vengono trattati da soggetti terzi: la tutela dei dati digitali diventa così uno strumento diretto di protezione dell'identità individuale. La nozione di *privacy* si amplia ulteriormente, includendo il diritto a non essere identificati o valutati esclusivamente sulla base delle informazioni diffuse, soprattutto quando queste vengono utilizzate fuori dal loro contesto originale. In questo senso, è corretto affermare che oggi la *privacy* assume una dimensione più ampia, estendendosi alla complessiva tutela dei dati personali e dell'identità del soggetto[77].

---

[73] D. RUGGIU, *Dalla profilazione al controllo: come ci manipola l'IA applicata alla politica*, Agenda Digitale, 2026, https://www.agendadigitale.eu/cultura-digitale/dalla-profilazione-al-controllo-come-ci-manipola-lia-applicata-alla-politica/.
[74] A. CAVARERO, *Il populismo digitale. L'illusione della democrazia diretta*, Rai Cultura, 2019, https://www.raicultura.it/filosofia/articoli/2019/01/Adriana-Cavarero-il-populismo-digitale-d2149873-58ed-442d-88a5-21bc90ac7aeb.html.
[75] S. DELLA PIAZZA, *Il caso Cambridge Analytica*, DirittoConsenso, 2021, https://www.dirittoconsenso.it/2021/12/21/il-caso-cambridge-analytica/.
[76] S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, Bologna, 2021 pp. 25-26.
[77] *Ivi*, p. 97.

Nella Carta dei diritti fondamentali dell'Unione europea, citata nel precedente capitolo, emerge una concezione ampliata dell'identità individuale, non più limitata alla dimensione fisica o psichica, ma estesa alla sfera informatica. Di fatto, assume rilievo l'idea di un'identità personale che si struttura anche attraverso l'insieme dei dati che riguardano l'individuo. Tale dimensione non rappresenta una realtà astratta o separata, bensì incide concretamente sulle relazioni sociali e sulla percezione di sé. L'insieme dei dati personali, organizzati e trattati attraverso strumenti tecnologici, diventa quindi un elemento essenziale attraverso cui l'individuo si colloca nel mondo contemporaneo. La progressiva emersione di questa consapevolezza ha condotto al riconoscimento di una protezione verso i propri dati personali, identificando un diritto autonomo, certamente distinto, rispetto alla tutela della vita privata, ma comunque strettamente connesso[78]. Questo diritto attribuisce all'individuo un ruolo attivo nella gestione delle informazioni che lo riguardano, accompagnandolo lungo l'intero ciclo della loro circolazione. In questa prospettiva, il problema centrale è quello di evitare che, l'identità personale venga interamente definita da soggetti terzi, i quali raccolgono e utilizzano i dati secondo logiche proprie. È così che nasce l'esigenza di garantire all'individuo un effettivo controllo sulla propria dimensione digitale, al fine di prevenire la perdita di autonomia nella costruzione della propria identità, superando i confini tradizionali della corporeità fisica e della sfera interiore. Tale legame si traduce in una serie di prerogative giuridiche, tra cui il diritto di accesso ai dati, la possibilità di verificare il trattamento secondo criteri di liceità e proporzionalità, nonché il potere di ottenerne l'eventuale cancellazione[79].

Tratto distintivo dell'identità personale è la sua naturale dinamicità, ossia la capacità di trasformarsi nel tempo; di fatti, si può affermare come questo interesse giuridico sia strettamente connesso al percorso evolutivo dell'individuo: esso si modifica in relazione alla crescita interiore, alle esperienze maturate, alle

[78] Il diritto alla protezione dei dati personali si distingue dal diritto all'identità personale in quanto non riguarda direttamente l'immagine sociale del soggetto, bensì il controllo sui dati.
[79] S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, Bologna, 2021, pp. 98-99.

eventuali contraddizioni e revisioni delle proprie convinzioni, rappresentando la proiezione esterna della propria personalità nella sua continua costruzione[80].

La progressiva centralità della dimensione informativa si accompagna a un ulteriore fenomeno caratteristico dall'ambiente digitale, rappresentato dalla moltiplicazione e frammentazione dell'identità personale. La diffusione di *Internet*, infatti, non incide soltanto sulle modalità di accesso e circolazione delle informazioni, ma determina anche una trasformazione della forma attraverso cui l'identità viene costruita o rappresentata. Anche storicamente l'identità poteva essere considerata non unitaria, ma articolata in relazione ai diversi contesti sociali; l'ambiente digitale amplifica tale frammentazione, offrendo una pluralità di spazi comunicativi nei quali l'individuo può presentarsi in modi differenti. La stessa persona si esprime attraverso molteplici canali, dando luogo a rappresentazioni diversificare e che talvolta, non sono pienamente coincidenti rispetto alla rappresentazione "reale", assumendo ruoli diversi o enfatizzando specifici aspetti della propria personalità. Nel caso dei profili *social*, ad esempio, il legame tra rappresentazione digitale e la persona è diretto e riconoscibile, risultando agevole configurare una lesione dell'identità personale, poiché l'interferenza incide direttamente sulla percezione pubblica dell'individuo[81]. Di fatto, la protezione dell'identità personale, non si estende alla mera possibilità di intervenire contro rappresentazioni inesatte sulla propria identità, ma anche, come forma di controllo sulla diffusione e sulla stessa elaborazione delle informazioni che riguardano l'individuo. Tale controllo emerge attraverso un sistema di garanzie procedurali che comprende, tra l'altro, l'obbligo di informare l'interessato, la richiesta del consenso per specifiche tipologie di trattamento, il diritto di correggere, aggiornare o eliminare dati non necessari, nonché la facoltà di opporsi al trattamento quando sussistano motivazioni legittime. Il rispetto di

[80] G. ALPA, G. RESTA, *Le persone fisiche e i diritti della personalità*, UTET Giuridica, 2006, pp. 102-103.
[81] G. FINOCCHIARO, *Identità personale (diritto alla)*, in *Digesto delle discipline privatistiche*, UTET, Torino, 2010, p.732.

queste regole costituisce il presupposto per la liceità del trattamento dei dati personali[82].

In questo senso, il contesto digitale ha mutato profondamento il significato di immagine, tradizionalmente intesa come mera rappresentazione della persona, creando così una concezione più ampia che include anche la dimensione digitale. L'immagine non si esaurisce più nella raffigurazione del soggetto, ma si estende all'insieme dei dati e delle rappresentazioni digitali che lo riguardano, stabilendo nuovi rischi derivanti dallo sviluppo delle moderne tecnologie.

1.1 Profilazione e raccolta dei dati

La crescente rilevanza dei dati personali nell'economia contemporanea ha dato origine a quello che viene comunemente definito "*data-driven-economy*", un modello economico in cui la creazione di valore si fonda sulla raccolta, l'analisi e l'utilizzo ingente di informazioni raccolte tramite le piattaforme *online*. Tali dati, spesso ceduti in modo apparentemente gratuito attraverso l'uso quotidiano di piattaforme digitali, alimentano processi di elaborazione che consentono alle imprese di prevedere comportamenti, preferenze e decisione degli utenti[83].

In questo contesto assume un ruolo centrale la profilazione. Con tale termine si intende l'insieme delle attività di raccolta e la successiva elaborazione dei dati relativi agli utenti, che vengono classificati in gruppi omogenei sulla base dei loro comportamenti, attraverso strumenti avanzati di analisi dei dati; tale definizione trova fondamento all'art. 4, punto 4 del GDPR[84].

La profilazione si fonda su diverse tecniche di raccolta dei dati, tra cui il cosiddetto "*footprinting* digitale", ossia l'insieme delle tracce informatiche che l'utente lascia durante la navigazione *online*, sia in modo attivo (come la

[82] G. PINO, *L'identità personale*, in S. RODOTÀ, M. TALACCHINI (a cura di), *Trattato di biodiritto*, vol. I, Giuffrè, Milano, 2010, p. 305.
[83] P. GALLO, *Intelligenza artificiale e protezione dei dati personali,* in *Digesto delle discipline privatistiche*, UTET, Torino, 2024 (aggiornato nel 2025), p. 3.
[84] «*Qualsiasi forma di trattamento automatizzato di dati personali consiste nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*».

condivisione di contenuti), sia in modo passivo (tramite indirizzi IP e dati di navigazione), costituendo la base primaria per le attività di profilazione. Tali tracce, infatti, contribuiscono in modo significativo alla costruzione della reputazione digitale dell'individuo. I *footprint* digitali rivestono un'importanza sempre più significativa, una volta immessi nello spazio digitale tendono ad avere una natura permanente e difficilmente controllabile dall'utente, come i dati condivisi in contesti che apparentemente sembrano privati. Il soggetto interessato perde il controllo sulla circolazione e il successivo utilizzo da parte di terzi, questo crea un pericolo anche su un altro livello: i contenuti possono essere decontestualizzati, fraintesi o alterati, generando potenziali effetti negativi sull'immagine e sulle relazioni personali. Informazioni inizialmente destinate a un pubblico ristretto possono inoltre diffondersi rapidamente a una platea molto più ampie e con conseguenze imprevedibili[85].

La disponibilità di grandi quantità di dati consente alle imprese, che ne detengono il controllo, di sviluppare rappresentazioni estremamente dettagliate degli utenti. Tali informazioni vengono impiegate per una pluralità di finalità, che spaziano dal *marketing* personalizzato fino a decisioni automatizzate sempre più rilevanti. In ambito commerciale, la pratica della profilazione, costituisce uno strumento imprescindibile per offrire sevizi personalizzati e comunicazioni pubblicitarie mirate, modellate sulle caratteristiche e sugli interessi dei singoli individui[86].

Un ulteriore ambito in cui l'utilizzo dei dati assume un ruolo centrale è rappresentato dall'addestramento dei sistemi di intelligenza artificiale[87], i quali si basano su grandi quantità di dati preesistenti per migliorare le proprie prestazioni. Tuttavia, l'utilizzo dei dati per l'addestramento dei sistemi di intelligenza

---

[85] *Che cos'è il footprint digitale? E come proteggerlo dagli hacker*, Kaspersky, https://www.kaspersky.it/resource-center/definitions/what-is-a-digital-footprint.

[86] Cfr. il considerato 24 del GDPR: «*Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali*».

[87] R. CASTROREALE, *Profilazione e Big Data: risvolti su privacy e sicurezza*, InSic, 2024. https://www.insic.it/privacy-e-sicurezza/information-security/profilazione-e-big-data-risvolti-su-privacy-e-sicurezza/.

artificiale si basa su informazioni già esistenti. Questo solleva importanti interrogativi poiché, se tali dati riflettono *bias*[88], disuguaglianze o pratiche discriminatorie già presenti nella società, tali distorsioni rischiano di essere replicate e amplificate dai sistemi di intelligenza artificiale[89]. Esempio emblematico è rappresentato dall'utilizzo dell'IA nei processi decisionali di assunzione del personale. L'automatizzazione di tali scelte, se non adeguatamente regolata e controllata, può condurre a esiti non etici o discriminatori, compromettendo principi fondamentali come l'equità e la trasparenza[90].

Per creare un ecosistema strutturato e organizzato, è importante attribuire un ruolo centrale ai *dataset*. Un *dataset* è un insieme organizzato di dati che costituisce la base informativa su cui vengono sviluppati e addestrati i modelli di intelligenza artificiale. Può contenere informazioni di natura diversa, come testi, immagini o valori numerici, strutturate in modo tale da essere interpretabili da un algoritmo[91]. La raccolta di tali dati può avvenire attraverso diverse modalità, tra cui il *web scraping*, ossia l'estrazione automatizzata di informazioni da siti *web*, archivi digitali o piattaforme *online* mediante *software* specifici[92]. Questa tecnica consente di acquisire grandi quantità di dati in tempi rapidi, risultando utile per la

---

[88] *«si riferisce al verificarsi di risultati distorti a causa di pregiudizi umani che alterano i dati di addestramento originali o l'algoritmo AI, portando a output distorti e potenzialmente dannosi»*, in J. HOLDSWORTH, *Che cos'è il bias AI?*, IBM, https://www.ibm.com/it-it/think/topics/ai-bias.

[89] P. GALLO, *Intelligenza artificiale e protezione dei dati personali*, in *Digesto delle discipline privatistiche*, UTET, Torino, 2024 (aggiornato nel 2025), p.10.

[90] Cfr. il caso *Amazon*, dove si evidenzia come l'utilizzo di strumenti di intelligenza artificiale nei processi di selezione del personale possa contribuire al rafforzamento di disuguaglianze di genere. Il sistema di reclutamento, addestrato su dati storici relativi alle assunzioni precedenti, caratterizzati da una prevalenza di candidati maschili, ha mostrato tendenze a penalizzare le candidature femminili, replicando *bias* già esistenti, in P. GALLO, *Intelligenza artificiale e protezione dei dati personali*, in *Digesto delle discipline privatistiche*, UTET, Torino, 2024 (aggiornato nel 2025), p.10.

[91] *AI per Open Source Datasets: Dati per l'Addestramento*, in Culture Digitali, https://culturedigitali.eu/notizie/ai-per-open-source-datasets-dati-per-laddestramento/.

[92] Cfr. il Garante per la protezione dei dati personali che ha rivolto particolare attenzione al fenomeno del *web scraping*, avviando nel dicembre 2023 un'indagine conoscitiva finalizzata a verificare se i gestori di siti pubblici e privati adottassero adeguate misure di sicurezza per prevenire la raccolta massiva dei dati, soprattutto in relazione all'utilizzo delle informazioni per addestrare sistemi di intelligenza artificiale. Il 30 maggio 2024, il Garante pubblica una nota informativa contenente prime indicazioni operative volte a favorire strumenti tecnici idonei a limitare l'estrazione automatizzate dei dati, in A. FUMAGALLI, *Web scraping: cos'è, perché si usa e come difendersi da "intrusioni" indesiderate*, Agenda Digitale, 2025, https://www.agendadigitale.eu/sicurezza/web-scraping-cose-perche-si-usa-e-come-difendersi-da-intrusioni-indesiderate/.

costruzione di *dataset* su larga scala. Infatti, durante la fase di addestramento, l'algoritmo viene esposto a numerosi esempi presenti nel *dataset* e, attraverso un processo iterativo, modifica i propri parametri interni per ridurre la distanza tra le proprie previsioni e i risultati corretti. In questo modo il modello apprende a riconoscere schemi ricorrenti, correlazioni e strutture implicite nei dati sviluppando capacità predittive o generative[93].

1.2 L'immagine nel mondo digitale: caso emblematico *CapCut*

Diversi sono gli interrogativi riguardo la posizione dell'immagine nel mondo digitale: che fine fanno realmente le fotografie, i video e i contenuti creativi che carichiamo sui canali *social* o sulle applicazioni di *editing*? Restano sotto il nostro controllo oppure, accentando condizioni contrattuali spesso lunghe e complesse, cediamo poteri molto più estesi di quanto immaginiamo? Chi può utilizzare quei contenuti? Possono essere modificati, distribuiti, ceduti o sfruttati economicamente da terzi, oltre che dall'applicazione principale? E, soprattutto, la cancellazione del profilo interrompe davvero ogni utilizzo, oppure i diritti già concessi continuano a produrre effetti?

Nel panorama digitale contemporaneo, il caricamento di immagini personali non rappresenta soltanto un atto di condivisione sociale, ma spesso costituisce l'ingresso di contenuti creativi e dati personali in un sistema economico che si fonda sulla monetizzazione e redistribuzione delle informazioni. Dal punto di vista giuridico, l'autore che carica immagini su piattaforme *online*, mantiene generalmente la titolarità sull'immagine o sul contenuto creato. In Italia, la tutela delle immagini è disciplinata dalla l. dir. aut., tutela che si estende anche ai contenuti diffusi sul *web*. La protezione nasce automaticamente nel momento della creazione dell'immagine[94]. Ciò significa che la paternità dell'opera, almeno formalmente, non viene automaticamente ceduta alla piattaforma con il semplice caricamento. Centrale è piuttosto la licenza d'uso che l'utente concede accettando

[93] *AI per Open Source Datasets: Dati per l'Addestramento*, in Culture Digitali, https://culturedigitali.eu/notizie/ai-per-open-source-datasets-dati-per-laddestramento/.
[94] A. DELLI PONTI, *Le immagini nel web: come usarle in modo legalmente corretto*, Studio Legale Delli Ponti, 2025, https://www.studiolegaledelliponti.eu/le-immagini-nel-web-come-usarle-in-modo-legalmente-corretto/#Immagini_e_fotografie_dal_web.

i Termini di Servizio[95]. Nella maggior parte delle piattaforme digitali, l'utente accorda una licenza molto estesa, compresa l'applicazione *CapCut*[96]. Si tratta di un caso emblematico per comprendere le dinamiche contemporanee di raccolta e utilizzo dei dati personali. Infatti, attraverso l'accettazione dei termini e delle condizioni d'uso, l'utente concede spesso autorizzazioni molto ampie sull'utilizzo dei contenuti caricati, che possono essere impiegate anche per finalità ulteriori rispetto alla semplice erogazione del servizio.

L'analisi di tale piattaforma consente di comprendere come i dati personali abbiano assunto un valore economico, diventando strumenti fondamentali per l'addestramento di sistemi di intelligenza artificiale e per lo sviluppo di tecnologie sempre più sofisticate. In questo caso l'immagine dell'individuo non rappresenta più soltanto un elemento della propria identità personale, ma diventa una risorsa utilizzabile dalle piattaforme digitali a fini commerciali e tecnologici. L'utente, spesso inconsapevolmente, contribuisce ad alimentare meccanismi di profilazione che consentono alle piattaforme digitali di accumulare enormi quantità di informazioni.

Nello specifico, i Termini di Servizio, di questa applicazione, dispongono quanto segue:

> *By submitting User Content via the Services, you grant to the Company and its affiliates a non-exclusive, royalty-free, transferable, sub-licensable, perpetual and worldwide licence to use your User Content*[97].

Questo sta a significare che la piattaforma può utilizzare, riprodurre, distribuire, modificare, pubblicare, creare opere derivate dai contenuti caricati dall'utente e sfruttare economicamente il contenuto per finalità commerciali, promozionali,

---

[95] *Il diritto d'autore delle immagini pubblicate su Internet e sui social media*, Studio Corradini, 2025, https://www.corradini.it/il-diritto-dautore-delle-immagini-pubblicate-su-internet-e-sui-social-media/.

[96] Applicazione del colosso tecnologico cinese, *ByteDance*, società madre anche di *TikTok*. Elemento particolarmente critico poiché i contenuti privati o realizzati possono essere distribuiti all'interno dell'ecosistema di *ByteDance*, in R. COLOMBO, *Ma li avete letti i nuovi termini d'uso di CapCut?*, Fotografi Digitali, 2025, https://www.fotografidigitali.it/news/ma-li-avete-letti-i-nuovi-termini-d-uso-di-capcut_140252.html.

[97] *CapCut Terms of Service*, ultimo aggiornamento 15 aprile 2026, https://www.capcut.com/clause/terms-of-service.

tecnologiche o algoritmiche, senza dover corrispondere compensi aggiuntivi all'autore. In alcuni casi, la licenza è estesa anche all'utilizzo dell'immagine personale o altri elementi identificativi per attività di *marketing* o di sviluppo di sistemi di intelligenza artificiale. Un'altra problematica riguarda la possibilità che determinati diritti siano trasferiti o subceduti a soggetti terzi, come, ad esempio, *partner* pubblicitari: in questo caso, la circolazione economica dei contenuti si amplia ben oltre l'intenzione originaria dell'autore. Formalmente, quindi, l'autore rimane titolare dell'opera, ma perde una parte significativa del controllo concreto dei dati personali caricati sulla piattaforma.

Ulteriore situazione di particolare rilevanza, è l'eventualità della cancellazione del profilo. Molti utenti ritengono che l'eliminazione del proprio *account* equivalga a revocare automaticamente ogni diritto precedentemente concesso, ma ciò non sempre corrisponde alla previsione contrattuale. Se i termini prevedono licenze perpetue e irrevocabili, i diritti già concessi possono continuare a sussistere anche dopo la cessazione del rapporto con la piattaforma, almeno per i contenuti precedentemente caricati. Nel caso preso in analisi, i termini di servizio prevedono che l'utente possa richiedere la cancellazione del proprio *account*, perdendo l'accesso ai contenuti caricati e ai dati associati. In termini pratici, anche se l'*account* viene eliminato, i diritti già attribuiti a *ByteDance*, possono continuare a produrre effetti.

Sul piano normativo il GDPR introduce tutele normative, imponendo trasparenza, correttezza e comprensibilità nelle informative e nelle condizioni di trattamento dei dati.

L'art. 12 del GDPR rubricato *"Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato",* sancisce quanto segue:

> *Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi*

elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

L'art. 7 presuppone come elemento fondamentale il consenso, e stabilisce che:

1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di prestare il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Qualsiasi parte delle condizioni che violi tali principi può risultare non vincolante. Inoltre, il consenso deve essere revocato con la stessa facilità con cui è stato prestato.

Però, nella pratica, tali garanzie non bastano, molte piattaforme continuano a utilizzare contenuti contrattuali complessi, caratterizzati da tecnicismi che rendono difficile per l'utente medio comprendere pienamente l'estensione dei diritti concessi.

Nel contesto dell'applicazione del GDPR e della tutela dei dati personali, le autorità di vigilanza rivestono un ruolo fondamente nel garantire che lo sviluppo e l'utilizzo delle tecnologie, sempre più invasive, avvengano nel rispetto dei diritti fondamentali degli individui. Il Regolamento, agli artt. 51,57,58, attribuisce alle autorità nazionali competenti il compito di controllare, prevenire e sanzionare

eventuali violazione della disciplina in materia di *privacy*. L'autorità nazionale competente è il Garante per la protezione dei dati personali (su cui v. infra, cap. 3).

Di particolare importanza, in questo senso, è stato il provvedimento adottato nei confronti di *OpenAI* e del servizio *ChatGPT*, attraverso il quale l'Autorità ha evidenziato le criticità legate alla raccolta e all'utilizzo dei dati personali. Il Garante ha ritenuto che il funzionamento del *software* violasse diversi principi fondamentali, contestando la raccolta e l'utilizzo massivo dei dati personali degli utenti; l'assenza di un'adeguata informativa sulla gestione dei dati (i dati venivano utilizzati senza un consenso esplicito e il trattamento appariva sproporzionato rispetto alle finalità dichiarate); l'assenza di strumenti efficaci per verificare l'età degli utenti minori di 13 anni. Il provvedimento ha avuto effetto immediato e ha imposto a *OpenAI* la limitazione provvisoria del trattamento dei dati degli utenti italiani[98].

Il controllo esercitato dalle autorità non rappresenta un limite alla tecnologia, bensì una garanzia democratica indispensabile, affinché l'intelligenza artificiale possa svilupparsi in modo sostenibile e conforme ai principi fondamentali.

2. *Machine learning*: basi teoriche per l'analisi del fenomeno dei *deepfake*

Nei paragrafi precedenti si è evidenziato come il ruolo dei dati sia centrale nello sviluppo dei sistemi di intelligenza artificiale. Comprendere l'importanza della raccolta dei dati e di come questi contribuiscano all'addestramento dei sistemi di intelligenza artificiale risulta essenziale per analizzare l'evoluzione di tecnologie sempre più avanzate, capaci di generare contenuti digitali sempre più realistici. Il progressivo perfezionamento di tali meccanismi consente di comprendere come l'intelligenza artificiale possa produrre rappresentazioni artefatte sempre più convincenti, riducendo la distanza tra contenuto generato e realtà. In questa prospettiva, analizzare il funzionamento dei sistemi di *machine learning* costituisce un passaggio fondamentale per introdurre e comprendere i fenomeni

[98] Garante per la protezione dei dati personali, *Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dei minori*, Garante Privacy, 2023, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847.

contemporanei; tra questi, i *deepfake*, che rappresentano una delle applicazioni più emblematiche della capacità generative raggiunte dall'intelligenza artificiale.

Il *machine learning* è un ramo dell'intelligenza artificiale che si concentra sullo sviluppo di algoritmi capaci di apprendere da un *set* di dati. Gli algoritmi, invece di essere programmati con istruzioni rigide, individuano autonomamente schemi all'interno dei dati di addestramento e utilizzano tali schemi per formulare previsioni o prendere decisioni su nuovi dati. Il principio fondamentale del modello di *machine learning* è che, se addestrato su dati rappresentativi del contesto reale, sarà in grado di generare e fornire risultati affidabili anche in situazioni nuove, trasferendo ciò che è stato appreso durante l'addestramento in scenari reali. All'interno del *machine learning*, il *deep learning* occupa un ruolo centrale. Esso si basa su reti neurali artificiali profonde, capaci di modellare relazioni molto complesse nei dati. Rispetto agli approcci tradizionali, queste tecniche permettono di raggiungere prestazioni elevate in diversi ambiti, ma richiedono una maggiore quantità di dati e notevoli risorse computazionali[99], come le GPU[100]. Questi modelli utilizzano parametri che vengono aggiornati tramite algoritmi di ottimizzazione, meccanismo che risulta ottimale per ottenere prestazioni elevati in molteplici ambiti, basti pensare alle generazioni di contenuti come immagini o testi[101].

[99] D. BERGMANN, *Cos'è il machine learning?*, IBM, https://www.ibm.com/it-it/think/topics/machinelearning#:~:text=Il%20machine%20learning%20%C3%A8%20il%20sottoinsieme%20dell'AI,per%20fare%20inferenze%20accurate%20sui%20nuovi%20dati.

[100] Una GPU (unità di elaborazione grafica) è specializzata nel gestire enormi quantità di calcoli matematici, in M. FLINDERS, S. SUSNJARA, I. SMALLEY, *Che cos'è un'unità di elaborazione grafica (GPU)?*, IBM, 2025, https://www.ibm.com/it-it/think/topics/gpu.

[101] D. BERGMANN, *Cos'è il machine learning?*, IBM, 2025, https://www.ibm.com/it-it/think/topics/machinelearning#:~:text=Il%20machine%20learning%20%C3%A8%20il%20sottoinsieme%20dell'AI,per%20fare%20inferenze%20accurate%20sui%20nuovi%20dati.

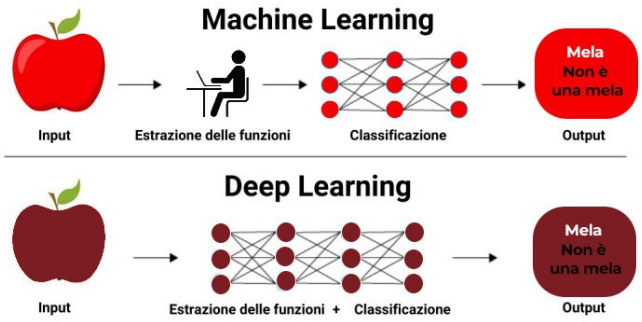

Figura 1: distinzione tra *machine learning* tradizionale e *deep learning* nella classificazione dei dati[102]

Un'importante classe di modelli generativi all'interno del *deep learning* è rappresentata dalle GAN (*Generative Adversarial Networks*). Si tratta di sistemi progettati per creare nuovi dati realisti, come immagini, audio o testi, apprendendo le caratteristiche da un insieme di dati già esistenti. Questa tecnica fu sviluppata nel 2014 dall'informatico Ian Goodfellow, con l'obiettivo di creare modelli in grado di generare nuovi dati a partire da quelli già esistenti. Per diversi anni il suo utilizzo rimase confinato nell'ambito della ricerca scientifica sull'intelligenza artificiale. Solo nel 2017 divenne noto al grande pubblico, quando un utente di *Reddit*, con lo pseudonimo di "*deepfake*", diffuse un video pornografico manipolato.

Le GAN operano tipicamente in un contesto di apprendimento non supervisionato e si basano su una struttura composta da due reti neurali che competono tra loro: il generatore e il discriminatore. Il primo produce dati sintetici a partire da *input* casuali, il secondo valuta i dati ricevuti e cerca di distinguerli tra quelli provenienti dal *dataset* e quelli generati artificialmente. Durante l'addestramento, il generatore migliora progressivamente la qualità dei dati prodotti cercando di ingannare il discriminatore, mentre quest'ultimo, affina la propria capacità di riconoscere i dati falsi. Questo processo competitivo porta entrambe le reti a evolversi fino a ottenere risultati sempre più realistici, il generatore produce

[102] La figura è tratta da V. LAVECCHIA, *Differenza tra deep learning e rete neurale*, Informatica e Ingegneria *Online*, 2021, https://vitolavecchia.altervista.org/differenza-tra-deep-learning-e-rete-neurale/. Il grafico mostra come i modelli di *machine learning* tradizionali abbiano bisogno di estrarre le caratteristiche in modo manuale, rispetto al modello di *deep learning* dove questa fase è integrata nella rete neurale (*v. op. ult. cit.*).

output sempre più convincenti, mentre il discriminatore diventa più sofisticato nel rilevare differenze sottili[103].

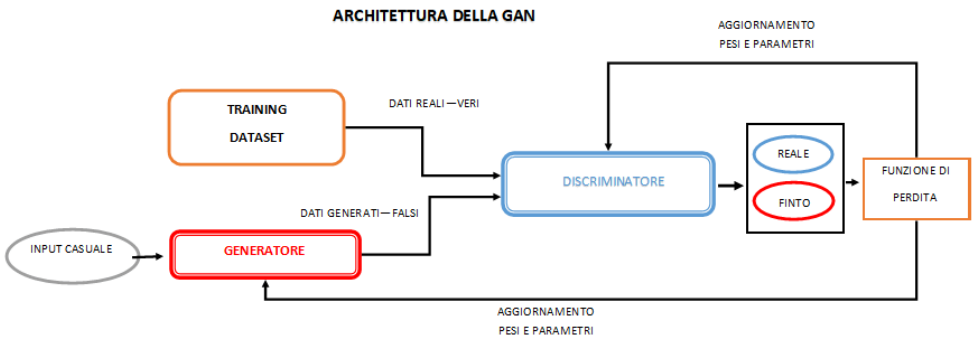

Figura 2: processi di addestramento dei sistemi GAN[104]

Nonostante i progressi raggiunti dal *machine learning* e in particolare dai modelli di *deep learning* come le GAN, emergono importanti criticità legate all'uso di queste tecnologie, capaci di generare contenuti sintetici estremamente realistici. Uno dei rischi più rilevanti è l'avvento dei *deepfake*, argomento di studio di questo elaborato. L'utilizzo sempre più facile di questi modelli fa sì che i rischi etici legati alle innovazioni portino sempre più incertezza riguardo alla veridicità dei contenuti con cui interagiamo quotidianamente.

2.1 *Deepfake*: nozione

Il Garante per la protezione dei dati personali ha formulato la seguente nozione di *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*[105].

---

[103] N. BASSETTI, *GAN (Generative Adversarial Networks): cosa sono, applicazioni e vantaggi*, Agenda Digitale, 2023, https://www.agendadigitale.eu/cultura-digitale/gan-generative-adversarial-networks-cosa-sono-applicazioni-e-vantaggi/.

[104] Figura tratta da N. BASSETTI, *GAN (Generative Adversarial Networks): cosa sono, applicazioni e vantaggi*, Agenda Digitale, 2023, https://www.agendadigitale.eu/cultura-digitale/gan-generative-adversarial-networks-cosa-sono-applicazioni-e-vantaggi/.

[105] Garante per la protezione dei dati personali, *Deepfake: dal Garante una scheda informativa sui rischi dell'uso malevolo di questa tecnologia*, 2020, Deepfake: dal Garante una scheda informativa sui rischi dell'uso... - Garante Privacy.

Il termine *deepfake*, di fatto, costituisce un neologismo: esso deriva da due parole inglesi: *"fake"*, comunemente traducibile come falso e *"deep"* in riferimento alle tecnologie di apprendimento profondo proprie dell'intelligenza artificiale, analizzate nel precedente paragrafo. Tali metodologie, sempre più sofisticate, consentono la manipolazione di contenuti audiovisivi quali immagini, registrazioni audio e video al fine di generare artefatti digitali verosimili. Le origini di tale fenomeno si rinvengono prevalentemente nel contesto della pornografia non consensuale, ove tali strumenti sono stati impiegati per la produzione e diffusione di materiali lesivi di dignità personale, frequentemente nell'ambito di pratiche di *revenge porn* o *sextortion*. Ancora oggi, una quota preponderante dei *deepfake* circolanti in rete è riconducibile a contenuti di natura pornografica non consensuale. Alla luce di tali evidenze, non sorprende come i *deepfake* vengano identificati come una minaccia emergente e di un certo spessore, basti pensare ai molteplici illeciti che a cascata un soggetto può commettere mettendo in circolo *deepfake*, quali: estorsioni, diffamazione, furti d'identità e frodi informatiche. Inoltre, esso si configura come nuova forma di disinformazione idonea a compromettere l'equilibrio dei sistemi democratici[106].

Esistono peraltro diversi modelli di *deepfake* ed il loro utilizzo non è necessariamente negativo.

Una prima tipologia è rappresentata dalla sincronizzazione labiale e dalla manipolazione dell'audio, tecnica che non si discosta troppo, nei risultati, da quelle tradizionalmente usate nel doppiaggio cinematografico. In questo caso, i movimenti della bocca di un soggetto vengono modificati per adattarsi a una traccia vocale alterata, creando l'illusione che la persona pronunci parole mai realmente dette. Un esempio noto di utilizzo positivo di questa tecnologia è stato quello dell'attore David Beckham, protagonista della campagna internazionale "*Malaria Must Die*" nel 2019, in cui, tramite tecnologie *deepfake*, appariva

[106] M. CAZZANIGA, *Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai deepfakes*, *MediaLaws, Rivista di diritto dei media*, 2023, pp. 172-174.

parlare in diverse lingue per sensibilizzare il pubblico globale sul tema della malaria[107].

Altra forma, probabilmente la più conosciuta, è il *face-swapping*, in cui il volto di una persona viene sovrapposto a quello di un'altra tramite reti neurali capaci di replicare espressioni facciali e movimenti in modo estremamente realistico. Nel settore cinematografico, un caso rilevante è quello di *Fast & Furious* 7, dove, dopo la morte dell'attore Paul Walker, il fratello Cody Walker è stato utilizzato come controfigura, mentre avanzate tecniche di CGI e *face replacement* hanno consentito di ricostruire il volto dell'attore, completando le scene mancanti.

Una terza categoria può essere costituita dai cosiddetti *deepfake* "*puppet-master*". In questa tecnica, le espressioni facciali e i movimenti vengono trasferiti in tempo reale su un altro soggetto presente in video o nell'immagine. Un individuo agisce come "regista" davanti a una telecamera, controllando dinamicamente le espressioni del volto del soggetto finale[108]. Diversamente dal *face-swapping*, dove viene sostituito il volto di una persona con quello di un'altra, mantenendo i movimenti originali del corpo e delle espressioni del soggetto, nel *puppet-master* vengono controllate o modificate le espressioni facciali e i movimenti del viso di una persona tramite quelli di un altro individuo. Caso di particolare rilevanza è rappresentato dal video, realizzato dal regista Jordan Peele, sull'ex presidente degli Stati Uniti, Barack Obama, dove appare pronunciare frasi mai dette realmente, tra cui insulti rivolti all'allora presidente Donald Trump.

Tali capacità di alterazione producono, dunque, effetti particolarmente invasivi sul piano dell'identità persona, compromettendo il controllo dell'individuo sulla propria immagine, sulla propria reputazione e dimensione psicologica. Sebbene tali strumenti fossero inizialmente impiegati nell'industria cinematografica e nella produzione di effetti speciali, la crescente accessibilità a *software* disponibili

[107] M. BUTCHER, *The startup behind that deep-fake David Beckham video just raised $3M*, TechCrunch, 2019, https://techcrunch.com/2019/04/25/the-startup-behind-that-deep-fake-david-beckham-video-just-raised-3m/.
[108] *Comprendere i diversi tipi di attacchi generativi AI Deepfake*, iProov, 2023, https://www.iproov.com/it/blog/generative-ai-attack-types-explained/.

anche su dispositivi di uso comune, ne ha favorito una diffusione capillare, ampliando in modo significativo il rischio di utilizzi illeciti[109].

La principale criticità risiede nel grado di veridicità che queste tecniche possono raggiungere sul piano tecnico. L'ampia diffusione e facilità di accesso contribuiscono a rendere sempre più labile il confine tra ciò che è reale e ciò che non lo è, fino a normalizzare una condizione di crescente sfiducia nelle informazioni, attribuendo di fatto un potere considerevole alla discrezionalità dei singoli individui che li utilizzano ed incidendo negativamente sul diritto all'informazione dei cittadini e sull'identità personale dei soggetti interessati.

2.1.1 Il fenomeno dei *deepnude*

Nel contesto dell'evoluzione normativa italiana contro gli abusi digitali legati all'intelligenza artificiale, un primo tentativo di regolamentazione risale al 2021 con la proposta di legge che mirava a introdurre l'art. 612-*quater* c.p., per punire la manipolazione artificiale di immagini di persone reali finalizzate alla creazione e diffusione di rappresentazioni nude senza consenso. Tale proposta nasceva per contrastare il fenomeno dei cosiddetti *deepnude*, una sottocategoria di *deepfake*, applicazioni capaci di "spogliare" digitalmente una persona attraverso algoritmi di intelligenza artificiale, generando immagini false ma realistiche, spesso utilizzate per umiliare o ricattare[110]. Sebbene questa proposta non sia stata ancora approvata nella sua formulazione originale, ha rappresentato un primo riconoscimento istituzionale del rischio giuridico e sociale posto da tali tecnologie.

È solo con la legge 23 settembre 2025 n. 132, che il legislatore italiano introduce una disciplina di protezione, inserendo nel Codice penale l'articolo 612- *quater*[111] rubricato "*illecita diffusione di contenuti generati o alterati con sistemi di*

[109] E. CHIZZOLA, *DEEPFAKE: tra furto d'identità, danno d'immagine e rischio privacy*, in Norme&Tributi Plus Diritto, Il Sole24Ore, 2021, https://ntplusdiritto.ilsole24ore.com/art/deepfake-furto-d-identita-danno-d-immagine-e-rischio-privacy-AE9Bowf.

[110] Camera dei deputati, *Introduzione dell'articolo 612-quater del Codice penale, in materia di manipolazione artificiale di immagini di persone reali allo scopo di ottenere rappresentazioni nude*, Scheda di lettura, 2021, https://documenti.camera.it/leg18/dossier/testi/gi0176.htm.

[111] «*Chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, è punito con la reclusione da uno a cinque anni*».

intelligenza artificiale". La norma punisce con la reclusione da uno a cinque anni chiunque diffonda, pubblichi o ceda immagini, video o voci falsificate o alterati mediante IA senza consenso, quando tali contenuti siano idonei a ingannate sulla loro autenticità e causino un danno ingiusto alla vittima. Questa formulazione estende la tutela non solo ai *deepnude*, ma anche alle forme di *deepfake* offensivi, inclusi video pornografici falsi, manipolazioni reputazionali e impersonificazione dannose[112]. La norma non va intesa come negazione assoluta della liceità dell'uso dell'intelligenza artificiale: la mera generazione di un *deepfake*, infatti, non integra di per sé un'ipotesi di illecito; la condotta ha carattere penale solo nel caso in cui il contenuto sia diffuso o condiviso con terzi senza il consenso della persona ritratta.

Ancora più allarmanti sono i casi che coinvolgono minori: solo nel 2025 sono stati individuati 8.213 minori vittime di *deepnude*, con un'evoluzione particolarmente allarmante sul panorama dello sfruttamento sessuale *online* di minori. Sempre più emergente per via di piattaforme digitali come *TikTok*, *Telegram*, *Signal* e aree più difficili da monitorale come il *Dark Web*. Secondo il *report* dell'Associazione *Meter*, il fenomeno si sta trasformando profondamente per via dell'integrazione di strumenti di intelligenza artificiale generativa sempre più facili da raggiungere. Sebbene le immagini siano generate digitalmente, il danno coinvolge sempre persone reali, alterando le immagini senza il consenso del diretto interessato, trasformando contenuti innocui in materiale sessualmente esplicito, costituendo una grave violazione dell'identità personale. Il crescente utilizzo dell'IA non sostituisce gli abusi, ma ne amplia il mercato, contribuendo alla normalizzazione e all'espansione della domanda di contenuti illegali. L'indagine dell'osservatorio Mondiale Contro la Pedofila, collegato a *Meter*, ha individuato almeno 115 gruppi e *bot* attivi su *Telegram* e *Signal* dedicati alla produzione e condivisione di *deepnude*. *Telegram* si conferma tra i principali canali di distribuzione, grazie alla sua struttura semi-anonima e alla facilità di creazione di gruppi privati. Tra gli strumenti tecnologici segnalati emerge l'utilizzo improprio di sistemi avanzati di

[112] A. CIRILLO, *Il nuovo reato: il Deepfake*, Studio Cataldi, il diritto quotidiano, 2026, https://www.studiocataldi.it/articoli/48017-il-nuovo-reato-il-deepfake.asp.

generazione immagini, incluso *Grok*[113], associato alla creazione di una parte significativa dei contenuti rilevati. Ogni contenuto individuato non rappresenta solo un dato statistico, ma la sofferenza reale di bambini e adolescenti che necessitano tutele sempre più concrete ed efficaci[114].

2.1.2 Le *fake news*

Le *fake news* generate attraverso tecnologie di *deepfake* rappresentano oggi una delle evoluzioni più pericolose della disinformazione digitale, poiché trasformano la tradizionale falsità informativa in contenuti audiovisivi dotati di una straordinaria forza persuasiva. A differenza delle *fake news* classiche, i *deepfake* sfruttano sistemi avanzati di intelligenza artificiale per creare video, audio o immagini in cui le persone reali appaiono pronunciare dichiarazioni o compiere azioni mai avvenute.

Questa capacità rende la manipolazione molto più credibile ed efficace sul piano psicologico, poiché il pubblico tende ancora a considerare immagini e video, prove più affidabili rispetto al semplice testo. La diffusione di contenuti artificiali non solo facilita la produzione di notizie false, ma erode il contesto stesso di prova audiovisiva, compromettendo la fiducia sociale ed alterando la percezione della realtà. In questo contesto, di particolare rilievo è l'art. 656 del Codice penale, che punisce la pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico. I *deepfake*, proprio per la loro capacità di manipolare la percezione di veridicità della notizia, possono rientrare in tali fattispecie.

Un esempio significato si è verificato durante il conflitto in Ucraina, quando sono circolati video falsi che simulavano dichiarazioni di pace attribuite ai presidenti Volodymyr Zelensky e Vladimir Putin. Se uno dei due è apparso poco credibile,

---

[113] Nuovo modello di intelligenza artificiale generativa, creata da xAI, società di Elon Musk, che sfrutta i dati raccolti tramite l'applicazione *X* (applicazione precedentemente conosciuta come *Twitter*), in *Che cos'è Grok: la nuova AI creata da Elon Musk*, Young Platform Academy, 2025, https://academy.youngplatform.com/tecnologia/che-cos-e-grok-la-nuova-ai-creata-da-elon-musk/.

[114] *L'agghiacciante report Meter sulla pedopornografia: oltre 8mila vittime di deepnude. Dagli 8 ai 12 anni i più colpiti*, Pro vita & Famiglia, 2026, https://www.provitaefamiglia.it/blog/lagghiacciante-report-meter-sulla-pedopornografia-oltre-8mila-vittime-di-deepnude-dagli-8-ai-12-anni-i-piu-colpiti#.

l'altro è risultato più persuasivo, dimostrando il crescente livello di queste tecnologie. In un contesto caratterizzato dalla cosiddetta "*post*-verità", diventa più difficile distinguere tra informazioni autentiche e manipolate. La situazione è resa ancora più complessa dal fatto che talvolta sono gli stessi politici a diffondere contenuti ingannevoli per screditare gli avversari. Caso esemplificato riguarda la diffusione da parte di Ron DeSantis di un'immagine manipolata che ritraeva Donald Trump in atteggiamenti affettuosi con Anthony Fauci, alimentando tensioni all'interno dell'elettorato repubblicano. Per contrastare tali fenomeni, alcuni Stati americani, tra cui California e Texas, hanno introdotto, nel 2019, norme che vietano la diffusione di *deepfake* nei 60 giorni precedenti alle elezioni, evitando l'interferenza con il corretto funzionamento dei sistemi democratici. A questo proposito, alcune delle piattaforme digitali hanno iniziato ad intervenire. Durante la pandemia di *COVID*-19 *YouTube* ha rimosso numerosi canali responsabili della diffusione di disinformazione sui vaccini; *Instagram* limita la visibilità dei contenuti segnalati come falsi; *Facebook* ha adottato misure per bloccare utenti che diffondono notizie ingannevoli[115].

Va inoltre considerato come la smentita di una notizia falsa risulta spesso meno efficace rispetto all'effetto della notizia stessa. Il contenuto iniziale, soprattutto se visivamente convincente, tende a diffondersi rapidamente, a differenza della correzione successiva. Questo squilibrio contribuisce ulteriormente alla pericolosità dei *deepfake* nel panorama informativo. Basti pensare al peso delle informazioni di rilevanza politica: in questo ambito, l'utilizzo dei *deepfake* può incidere in modo significativo sulla formazione dell'opinione pubblica, influenzando orientamenti elettorali.

2.3 L'evoluzione dei *deepfake* e degli strumenti per il riconoscimento delle manipolazioni

L'evoluzione dei deepfake ha seguito un percorso di rapido perfezionamento, trasformandosi da una tecnologia inizialmente caratterizzata da evidenti imperfezioni visive a uno strumento capace di produrre contenuti altamente realistici e difficili da distinguere dai contenuti originali. La creazione di un

[115] V. AZZALI, N. ELLECOSTA, *La questione deepfake in Italia: una panoramica*, *MediaLaws*, *Rivista di Diritto dei Media*, 2024, pp. 78-81.

deepfake richiede necessariamente l'individuazione di un volto da sovrapporre al soggetto originale. Ecco perché le vittime più comuni di queste manipolazioni sono spesso personaggi pubblici o celebrità: tali soggetti rappresentano bersagli ideali, non solo per l'elevato interesse che suscitano presso il pubblico *online*, ma soprattutto perché la realizzazione di *deepfake* veritieri necessita di una vasta quantità di dati biometrici. Le figure pubbliche, grazie alla costante esposizione mediatica, offrono una vasta disponibilità di immagini e video reperibili *online*; questa abbondanza di materiale facilita enormemente la costruzione di modelli facciali, rendendo le celebrità particolarmente vulnerabili all'utilizzo illecito della propria immagine nei processi di manipolazione sintetica.

A questo proposito sono stati condotti diversi studi per i progressivi miglioramenti tecnologici e il crescente impatto dei sistemi di *deepfake*. In particolare, nel presente elaborato si prenderà in esame lo studio condotto dall*'Universidad Autonoma de Madrid*, che ha evidenziato come le più recenti innovazioni tecnologiche abbiano reso i nuovi *deepfake* quasi impercettibile rispetto al contenuto autentico, attraverso l'impiego di tecniche sempre più all'avanguardia. Lo studio ha distinto l'evoluzione dei *deepfake* in due differenti generazioni: la prima generazione risultava maggiormente riconoscibile, sia dagli utenti, sia dai *software* di *detection*, poiché presentavano caratteristiche tecniche che rendevano poco realistiche i risultati finali come: volti sintetici di bassa qualità, differenze cromatiche tra la pelle artificiale e quella reale, residui del volto originale e limitate variazioni di posa. Questi limiti tecnici rendevano i contenuti manipolati facilmente rilevabili sia dall'occhio umano che dai sistemi automatici di rilevamento. Con il passaggio alla seconda generazione, numerose debolezze strutturali sono state significatamene ridotte. Lo studio dimostra come i nuovi *dataset* (*Celeb*-DF e DDFDC), introducano volti con qualità superiore, fusioni più naturali, migliori dettagli facciali e scenari più complessi, comprendenti variazione di luce, ambienti interni ed esterni, pose dinamiche e differenti distanze dalla telecamera[116]. L'analisi dimostra che il miglioramento qualitativo ha

[116] R. TOLOSANA, S. ROMEO-TAPIADOR, J. FIERREZ, R. VERA-RODRIGUEZ, *Deepfake Evolution: Analysis of Facial Regions and Fake Detection Performance*, airXiv, 2020, p. 1, https://arxiv.org/abs/2004.07532.

riguardato specifiche aree del volto, come naso, bocca e contorni facciali, rendendo le anomalie sempre più difficili da identificare. Non solo, i costanti miglioramenti dimostrano come ci sia una crescita di realismo esorbitante, portando ad eludere persino i *software* di *detection*[117].

L'Università di Buffalo, sotto la guida del ricercatore Siwei Lyu, ha sviluppato *Deepfake-o-Meter*, un *software open-source* progettato per supportare il riconoscimento di contenuti manipolati. La piattaforma, accessibile previa semplice registrazione, consente di verificare l'autenticità di audio, immagine e video sospetti caricandoli direttamente nel sistema. Il programma restituisce una valutazione probabilistica, espressa in percentuale, circa la possibilità che il contenuto analizzato sia stato creato artificialmente, lasciando all'utente la valutazione conclusiva. Questo approccio, basato su un'analisi non binaria, rappresenta un importante progresso nelle strategie di contrasto alla disinformazione digitale. Il ricercatore sottolinea, però, come tale tecnologia da sola non possa garantire una protezione assoluta, ma è necessario sviluppare un pensiero critico che porti l'utente a interrogarsi sulla veridicità del contenuto[118].

Dal punto di vista tecnico, la Polizia Postale evidenzia come alcuni piccoli segnali possano aiutare a riconoscere un video creato con l'intelligenza artificiale: spesso nella realizzazione di un *deepfake* viene dedicata maggiore cura al volto, mentre risultano trascurati elementi come la postura del corpo, le luci e le ombre. Anche il movimento degli occhi, il battito delle ciglia, la definizione dei denti e la perfetta sincronizzazione tra voce e labbra sono aspetti particolarmente difficili da riprodurre in modo realistico. È importante controllare con attenzione l'autorevolezza della fonte, verificare se l'informazione è riportata anche da altri canali affidabili e analizzare la presenza di eventuali elementi riconducibili all'uso delle tecniche di intelligenza artificiale[119].

---

[117] *Ivi*, p. 2.
[118] F. M. BARBUTO, *Adesso una piattaforma online permette di smascherare i deepfake*, E-Campus Blog, 2024 https://blog.uniecampus.it/2024/10/01/deepfake-o-meter-un-programma-per-smascherare-i-deepfake/.
[119] Polizia Postale, *Come riconoscere un deepfake*, Commissariato di PS *Online*, 2024, https://www.commissariatodips.it/notizie/articolo/come-riconoscere-un-deepfake/index.html.

In tale senso, bisogna specificare come, il fenomeno dei *deepfake* non si colloca come tema autonomo rispetto al diritto all'immagine, ma piuttosto come nuova modalità di lesione dei diritti della personalità. L'impiego di tali tecnologie, rende necessario riesaminare le tradizioni categorie giuridiche elaborate dal legislatore, evidenziando la necessità di adattare gli strumenti di tutela esistenti alle nuove forme di manipolazione dell'immagine.

CAPITOLO III
RIMEDI NORMATIVI E TUTELE CIVILISTICHE

1. L'approccio europeo ai rischi dell'ecosistema digitale: il *Digital Services Act* e *Artificial Intelligence Act*

Giunti a questo punto dell'indagine, prima di addentrarsi negli strumenti di tutela civilistica, diventa necessario un approfondimento delle normative europee volte a garantire una maggiore tutela nell'ambiente digitale. L'Unione europea, infatti, è tra i primi attori internazionali ad aver introdotto strumenti normativi per regolare i sistemi di intelligenze artificiali nell'ecosistema di rete. In tale contesto, accanto agli strumenti più generali sopra citati, risultano centrali il *Digital Services Act*[120], volto a disciplinare le responsabilità delle piattaforme *online* e a rafforzare la tutela degli utenti nello spazio digitale, e l'*Artificial Intelligence Act*[121], prima disciplina organica globale in materia di intelligenza artificiale, finalizzata a garantire un utilizzo sicuro e trasparente, rispettoso dei diritti fondamentali. Si tratta di normative che cercano di rispondere a fenomeni in continua evoluzione, caratterizzati da un rapido sviluppo e da nuove forme di rischio per gli utenti e per la società nel suo complesso.

Il *Digital Services Act* (DSA) e il *Digital Markets Act* (DMA)[122] sono due Regolamenti dell'Unione europea adottati dal Parlamento europeo il 5 luglio 2022. Essi costituiscono il cosiddetto *Digital Services Package*, cioè un insieme di norme volto a disciplinare il mercato digitale europeo. L'obiettivo principale è quello di garantire il funzionamento dell'ambiente digitale dell'Unione, tutelare i consumatori ed evitare la disinformazione *online*, entrambi i Regolamenti sono entrati in vigore nel 2022 e sono divenuti applicabili alle piattaforme *online* dal 17 febbraio 2024. Nello specifico, il *Digital Services Act*, disciplina una serie di

[120] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).
[121] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).
[122] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).

servizi digitali che svolgono funzioni di intermediazione tra utenti e contenuti immessi in rete. L'ambito di applicazione del DSA comprende, quindi, tutti gli intermediari digitali e le piattaforme *online* che offrono servizi nel mercato dell'Unione europea, tra cui *marketplace*, *social media*, piattaforme per la condivisione di contenuti, *app store* e piattaforme di viaggio e alloggio *online*[123]. Lo scopo primario è quello di estendere ancora di più le tutele degli utenti in ambito di trasparenza e sicurezza *online*; inoltre, l'idea è quella di rendere l'ambiente digitale più sicuro, gestendo in modo più efficace i contenuti illegali[124], compresi quelli che amplificano la proliferazione di odio e di disinformazione. A questo proposito, le piattaforme, devono implementare i sistemi di controllo dei contenuti, evitando che la libertà d'espressione, diventi un'arma dannosa[125].

Oltre a implementare le misure di tutela in ambito di trasparenza e responsabilità, il regolamento prevede strumenti per contrastare i contenuti illeciti, tra cui sistemi di segnalazione che coinvolgono enti qualificati che collaborano con le piattaforme per individuare contenuti illegali: i *trusted flaggers*. Altro elemento della normativa è quello della trasparenza degli algoritmi, soprattutto per quanto concerne la personalizzazione dei contenuti e della pubblicità. Il sistema normativo è implementato da codici di condotta e *standard* tecnici, che si propongono di uniformare il più possibile la disciplina applicata a livello comunitario. Le norme si applicano agli intermediari che operano nel *marketplace* europeo, indipendentemente dal Paese della sede legale[126].

Il regolamento prevede un articolato sistema sanzionatorio per le piattaforme che non rispettano gli obblighi stabiliti, con scopo di assicurare l'applicazione concreta ed efficace delle disposizioni presenti nel DSA. Le violazioni più gravi

---

[123] *Legge sui servizi digitali: Domande e risposte*, Shaping Europe's digital future, 2025, https://digital-strategy.ec.europa.eu/it/faqs/digital-services-act-questions-and-answers.

[124] Cfr. art. 3 lett. h) DSA: «*«contenuto illegale»: qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto*».

[125] G. CONTISSA, F. GALLI, *La governance della "disinformazione aumentata" tra Digital Services Act e AI Act*, Federalismi, n. 15, 2025, pp. 133-134.

[126] *Ivi*, pp. 136-137.

possono determinare l'applicazione di sanzioni amministrative fino al 6% del fatturato annuo mondiale dell'impresa interessata, per inadempimenti legati alla trasmissione di informazioni non esatte o fuorvianti; per il mancato rispetto degli obblighi sulla trasparenza e cooperazione, invece, si applica una percentuale pari all'1% del fatturato annuo globale[127]. L'aspetto più importante nell'applicazioni delle sanzioni, oltre che sul piano deterrente, si estende alla tutela dell'utente, al quale viene riconosciuta la possibilità di ottenere un risarcimento qualora subisca danni derivanti dalla violazione di tale regolamento[128].

L'attuazione del DSA si fonda su un modello multilivello, che è presenziato dalla cooperazione delle istituzioni europee e dalle autorità nazionali. Ruolo centrale è svolto dalla Commissione europea, cui compete la supervisione delle piattaforme e motori di ricerca *online* di dimensioni molto grandi, nello specifico quelle che superano 45 milioni di utenti attivi nell'Unione europea, possedendo poteri sia sul lato investigativo che sanzionatorio. Non solo, la Commissione verifica se le piattaforme abbiano adottato misure efficaci per contrastare i rischi sistematici dell'ambiente digitale. Le piattaforme di minori dimensioni sono soggette alla vigilanza delle autorità nazionali competenti degli Stati membri in cui hanno sede. Il Regolamento prevede, infatti, che ciascuno Stato membro designi un coordinatore dei Servizi Digitali, incaricato di vigilare sull'applicazione delle disposizioni previste dalla normativa. Nel caso di violazioni con effetti transfrontalieri, le autorità nazionali riportano alla Commissione l'infrazione, mentre il coordinatore dello Stato membro assume il coordinamento delle indagini. È previsto anche il *Compliance Officer*, figura interna alle piattaforme di maggiori dimensioni incaricata di monitorare il rispetto della normativa e di rispettare gli obblighi del regolamento. A livello sovranazionale, svolge un ruolo di particolare rilevanza il Comitato europeo per i servizi digitali, presieduto dalla Commissione europea. Esso ha il compito di promuovere il coordinamento e la

[127] Art. 52, paragrafo 3, DSA.
[128] B. CALDERINI, *Digital Services Act: cos'è e cosa prevede la legge europea sui servizi digitali*, Agenda Digitale, aggiornato nel 2025, https://www.agendadigitale.eu/mercati-digitali/digital-services-act-cose-e-cosa-prevede-la-legge-europea-sui-servizi-digitali/.

cooperazione degli Stati membri, per assicurare un'applicazione omogenea del regolamento all'interno del territorio comunitario[129].

Nonostante la struttura normativa rigorosa, le disposizioni previste dal DSA sono di difficile applicazione, anche per la mancata cooperazione delle piattaforme cui la normativa è diretta. Soprattutto gli operatori digitali dispongono, infatti, di considerevoli mezzi economici e legali, che sono utilizzati spesso per contrastare le decisioni delle istituzioni europee, ostacolando l'*enforcement* delle istituzioni[130][131].

Quando un contenuto disinformativo è considerato illecito, il prestatore di servizi può essere esonerato da responsabilità solo se interviene rapidamente dopo una segnalazione effettuata dagli utenti o una notifica dell'autorità competente. In quest'ultimo caso, l'art. 9 del DSA impone ai fornitori di servizi di cooperare con gli Stati membri, predisponendo appositi punti di contatto dando esecuzione agli ordini di rimozione. Il DSA introduce inoltre un sistema che consente agli utenti di segnalare contenuti illegali tramite notifiche motivate e sufficientemente dettagliate. Se la segnalazione soddisfa i requisiti previsti, il prestatore acquisisce conoscenza dell'illiceità del contenuto e deve intervenire prontamente per limitante la diffusione o la rimozione[132][133].

Il contenuto disinformativo può essere soggetto alle disposizioni del DSA, non solo quando viene qualificato come illecito dal diritto dell'Unione o dalla

---

[129] *Ibidem*.

[130] *Ibidem*.

[131] Sul punto, si veda: *La Commissione infligge ammende per un importo di 120 milioni di EUR a norma della legge sui servizi digitali*, Shaping Europe's digital future, 2025, dove la Commissione Europea ha inflitto a X una sanzione pecuniaria di 120 milioni di euro. Provvedimento scattato a seguito del mancato rispetto degli obblighi di trasparenza previsti dal DSA. Le contestazioni principali riguardano nello specifico: il sistema ingannevole delle "spunte blu"; mancanza di trasparenza del *repository* di annunci; mancata fornitura ai ricercatori dell'accesso ai dati pubblici.

[132] L'art. 16 DSA rubricato "*Meccanismo di segnalazione e azione*" prevedere al paragrafo 1 che: «*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*».

[133] G. CONTISSA, F. GALLI, *La governance della "disinformazione aumentata" tra Digital Services Act e AI Act*, Federalismi, n. 15, 2025, p. 136.

normativa nazionale, ma anche nel caso in cui contrasti con le condizioni e le regole stabilite dalla piattaforma digitale[134]. Nel caso di una decisione di rimozione o limitazione adottata da sistemi automatizzati, l'art. 17 del DSA prevede l'obbligo di fornire una motivazione chiara della decisione, per questioni di trasparenza. L'art. 20 introduce un sistema di reclamo che garantisce l'intervento umano nella revisione delle decisioni contestate. Il DSA cerca quindi, di rafforzare le garanzie di trasparenze e tutela degli utenti rispetto ai processi automatizzati[135].

Nel complesso, il DSA non prevede un esplicito riferimento ai *deepfake*, ma alcune disposizioni presenti nel Regolamento risultano strettamente connesse. Nello specifico, il DSA impone alle piattaforme *online* e ai motori di ricerca di estese dimensioni l'obbligo di effettuare valutazione dei rischi sistematici derivati dai propri servizi, adottando misure adeguate ed efficaci per prevenire gli effetti negativi sul dibattito pubblico e sui processi democratici ed elettorali. Tale previsione appare rilevante con riguardo ai *deepfake* utilizzati ai fini della disinformazione politica, nonché alla necessità di assicurare un'adeguata identificazione ed etichettatura dei contenuti generati o alterati mediante sistemi di intelligenza artificiale[136].

Particolare attenzione è stata dedicata ai rischi derivanti dall'impiego dell'intelligenza artificiale generativa. I motori di ricerca e le piattaforme *online* che consentono la produzione e la diffusione di contenuti creati mediante IA, devono individuare preventivamente i possibili rischi connessi a tali strumenti, adottando misure adeguare per limitare gli effetti negativi, come l'obbligo di rendere chiaramente riconoscibili i contenuti manipolati[137].

La normativa europea in materia di protezione dai rischi derivanti dal mondo digitale non si esaurisce con la disciplina precedentemente richiamata, ma trova

---

[134] *Ivi*, p. 138.
[135] *Ivi*, p. 140.
[136] A. ORLANDO, *La regolamentazione del deepfake in Europa, Stati Uniti e Cina*, *MediaLaws, Rivista di diritto dei media,* 2025, p. 313, https://www.medialaws.eu/wp-content/uploads/2025/02/I-24-Orlando.pdf.
[137] G. CONTISSA, F. GALLI, *La governance della "disinformazione aumentata" tra Digital Services Act e AI Act*, Federalismi, n. 15, 2025, p. 143.

ulteriore sviluppo nell'ambito dell'intelligenza artificiale attraverso l'*Artificial Intelligence Act*, adottato tramite Regolamento (UE) 2024/1689. Tale normativa, proposta dalla Commissione europea nel 2021 e successivamente approvata dal Parlamento europeo e dal Consiglio nel dicembre 2023, rappresenta il primo quadro normativo mondiale volto a disciplinare l'utilizzo dei sistemi di intelligenza artificiale. Il regolamento è entrato ufficialmente in vigore il 1° agosto 2024, con un periodo di transizione di 6-36 mesi[138], con lo scopo di garantire un utilizzo dell'IA più sicuro e conforme ai diritti fondamentali dell'individuo[139].

Nello specifico, la normativa introduce una classificazione dei sistemi di intelligenza artificiale secondo quattro livelli, determinati in funzione del livello di rischio. La prima categoria comprende i sistemi considerati a rischio inaccettabile. Il secondo livello comprende invece i sistemi ad alto rischio. Una terza categoria riguarda i sistemi caratterizzati da un rischio limitato. Infine, i sistemi classificati per il loro rischio minimo. La normativa introduce una disciplina autonoma per i modelli di IA a finalità generali, che prevede obblighi più rigorosi per sistemi di IA a scopo generale a rischio sistematico[140]. Il legislatore europeo ha previsto nel regolamento strumenti specifici diretti a limitare gli effetti negativi della disinformazione, nello specifico, se diffusa attraverso strumenti digitali avanzati, come l'IA generativa[141].

Il paragrafo 60 dell'art. 3 dell'*AI Act* fornisce esplicitamente la definizione di *deepfake*:

> *«deep fake»: un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona.*

[138] Nello specifico: le disposizioni riguardanti l'alfabetizzazione in materia di intelligenza artificiale, insieme ai relativi divieti e alle definizioni previste sono entrate in vigore il 2 febbraio 2025; le norme relative alla *governance* dell'IA e gli obblighi applicabili ai modelli di intelligenza artificiale per finalità generali, sono operative dal 2 agosto 2025; i sistemi di IA classificati come ad alto rischio, diventeranno applicabili dopo il periodo transitorio di 36 mesi dall'entrata in vigore del Regolamento, ossia a partire dal 2 agosto 2027. In *Navigazione della legge sull'IA*, EU Digital Strategy, 2026, https://digital-strategy.ec.europa.eu/it/faqs/navigating-ai-act.
[139] *Entra in vigore il regolamento sull'IA*, COMMISSIONE EUROPEA, 2024, https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_it.
[140] G. CONTISSA, F. GALLI, *La governance della "disinformazione aumentata" tra Digital Services Act e AI Act*, Federalismi, n. 15, 2025, pp. 145-146.
[141] *Ivi*, p. 146.

Questa definizione, si fonda su diversi requisiti che rendono l'interpretazione complicata. In particolare, ai fini della qualificazione del carattere manipolatorio del contenuto, risulta necessario stabilire quando un materiale possa essere qualificato come *deepfake*. Nel caso dell'immagine, va considerato che una fotografia non rappresentata in modo vero la realtà, ma deriva da una serie di processi digitali e da scelte effettuate in fase di acquisizione e *post*-produzione. Ad esempio, occorre valutare se i filtri basati su sistemi di IA possano integrare una forma di manipolazione tale da far rientrare l'immagine nella nozione di *deepfake*, purché ricorrano gli ulteriori requisiti richiesti dalla normativa. Non è ancora chiaro quale grado di somiglianza con contenuti reali sia richiesto ai fini della qualificazione di un contenuto come *deepfake*. In particolare, ci si interroga se sia necessario che il contenuto riproduca in modo riconoscibile un soggetto realmente esistente oppure possa essere qualificato come *deepfake* anche un volto generato sinteticamente, qualora esso sia comunque idoneo a essere associato a un individuo identificabile. Infine, rispetto alla capacità di indurre in errore la percezione umana, la formulazione sembra escludere i casi in cui l'inganno si verifichi unicamente nei confronti di sistemi automatizzati, senza che vi sia un effettivo inganno per un osservatore[142].

L'art. 50 al paragrafo 4 dell'*AI Act* dispone che:

> *I deployer*[143] *di un sistema di IA che genera o manipola immagini o contenuti audio o video che costituiscono un «deep fake» rendono noto che il contenuto è stato generato o manipolato artificialmente. Tale obbligo non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare o perseguire reati. Qualora il contenuto faccia parte di un'analoga opera o di un programma manifestamente artistici, creativi, satirici o fittizi, gli obblighi di trasparenza di cui al presente paragrafo si limitano all'obbligo di rivelare l'esistenza di tali contenuti*

[142] *Ivi*, pp. 149-150

[143] Per *deployer* si intende il soggetto, privato o pubblico, che utilizza un sistema di intelligenza artificiale nell'esercizio della propria attività. Restano esclusi gli utilizzi effettuati per scopi esclusivamente personali e privi di carattere professionale. Cfr. S. STEFANELLI, *AI Act e responsabilità penale: cosa cambia per provider e deployer*, Agenda Digitale, 2024, https://www.agendadigitale.eu/sicurezza/privacy/ai-act-e-responsabilita-penale-cosa-cambia-per-provider-e-deployer/#:~:text=Il%20deployer%20%C3%A8%20invece%20la,'attivit%C3%A0%20personale%20non%20professionale%E2%80%9D.

generati o manipolati in modo adeguato, senza ostacolare l'esposizione o il godimento dell'opera […].

I soggetti che utilizzano sistemi di IA per creare o alterare contenuti manipolati, sia che siano audio, video o immagini, sono tenuti a informare gli utenti che tali contenuti sono stati generati o modificati artificialmente. Sono tuttavia previste alcune deroghe, in particolare quando gli strumenti di manipolazione vengono impiegati per finalità legittime, come le indagini penali, oppure in ambito artistico o di intrattenimento. In tali casi l'obbligo di trasparenza si traduce nella necessità di fornire un'informazione adeguata che non comprometta la fruizione o la qualità del contenuto. La finalità della disciplina è quella di bilanciare interessi contrapposti, tra cui, la tutela della trasparenza e la salvaguardia della libertà d'espressione. Inoltre, chi utilizza sistemi di IA per generare o manipolare testi destinati a informare il pubblico su questioni di interesse generale è tenuto a rendere noto che tali contenuti sono stati prodotti o modificati mediante l'impiego dell'intelligenza artificiale[144].

L'*AI Act* non vieta esplicitamente la creazione di *deepfake*, ma l'art. 5, paragrafo 1 prevede un divieto di alcune tipologie di pratiche di IA tra cui, alla lettera a):

L'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo.

Un ruolo importante è rivestito, poi, dalle Linee Guida e in particolare dal paragrafo 71, che affronta il tema della trasparenza a proposito di contrasto contro le tecniche manipolative dell'intelligenza artificiale. Nello specifico, il paragrafo si propone di evidenziare come l'identificazione delle *chatbot* e dei contenuti *deepfake* costituisca un prerequisito essenziale per mitigare i rischi connessi

[144] *Ivi*, p. 149.

dall'utilizzo dell'IA generativa. Senza tale presidio, la diffusione di elementi artificiali rischia di generare pericolose distorsioni rispetto alla realtà, capaci di influenzare negativamente gli utenti nelle loro convinzioni personali e nelle loro condotte. Il quadro normativo introduce tutele più stringenti attraverso regimi di divieti assoluti. È essenziale, a questo proposito, richiamare l'art. 5, paragrafo 1 lettera b) del Regolamento che vieta l'impiego di sistemi di IA progettati per sfruttare deliberatamente le fragilità di categorie specifiche che sia legata all'età, alle disabilità a condizioni di svantaggio socioeconomiche[145].

Il DSA e l'AI Act costituiscono due ecosistemi normativi centrali per la regolamentazione digitale. L'elaborazione dei due Regolamenti si basa su strumenti regolatori differenti e su piani distinti, anche se entrambi, seppur in maniera diretta, incidono sul fenomeno della "disinformazione aumentata". I due Regolamenti hanno delle finalità comuni, come: la protezione dei diritti fondamentali, il rafforzamento della trasparenza e la prevenzione dei rischi derivanti dall'impiego delle informazioni digitali[146]. D'altra parte, sebbene entrambe le normative si inseriscano nel medesimo contesto digitale, non seguono logiche regolatorie omogenee, circostanza che potrebbe determinare aree di interferenza, vuoti normativi oppure difficoltà interpretative nella loro concreta applicazione[147].

Tale possibile disallineamento tra le due normative sembra essere riconosciuto dallo stesso *AI Act*. In particolare, i considerando 120 e 136 evidenziano come gli obblighi imposti ai fornitori e agli utilizzatori di determinati sistemi di IA, soprattutto quelli relativi all'identificazione dei contenuti generati o manipolati artificialmente assumono rilievo anche ai fini dell'applicazione del DSA. Tuttavia, poiché tali indicazioni sono contenute esclusivamente nei considerando e non nelle disposizioni normative vincolanti, permane incertezza interpretativa circa l'effettivo rapporto tra le due discipline e le loro modalità di coordinamento. Resta aperto a questo proposito il quesito se il rispetto degli obblighi previsti

[145] G. CONTISSA, F. GALLI, *La governance della "disinformazione aumentata" tra Digital Services Act e AI Act*, Federalismi, n. 15, 2025, p. 147.
[146] *Ivi*, p. 152.
[147] *Ibidem*.

dall'*AI Act* possa essere sufficiente ai fini della conformità con il DSA, oppure se le due discipline debbano essere applicate separatamente. Inoltre, non è chiaro se tale coordinamento riguardi tutti gli eventuali obblighi relativi alla disinformazione oppure si circoscriva soltanto ai modelli di IA a uso generale e alla gestione dei rischi sistematici. Le conseguenze di queste incertezze si espletano sulla distribuzione delle responsabilità, soprattutto nel caso dell'IA generativa e quando queste ultime vangano utilizzate attraverso piattaforme *online* accessibile ad un vasto pubblico. Nel concreto, le difficoltà, soprattutto nel contesto della responsabilità, riguardano in particolare allo stabilire chi sia il responsabile della diffusione di contenuti disinformativi: il fornitore del sistema di IA, il gestore della piattaforma o l'utente che lo utilizza. Sebbene gli obiettivi dei Regolamenti siano simili, la loro applicazione richiede un coordinamento più esplicito e chiaro, per scongiurare il rischio di sovrapposizioni normative e incertezze che si estendono a tutti i soggetti coinvolti[148].

2. Il Garante per la protezione dei dati personali

Lo scopo dei Regolamenti sopra citati, è quello di introdurre una disciplina uniforme nell'ambiente comunitario. In tale contesto, assumono ruolo centrale le autorità competenti chiamate a vigilare sul rispetto e sulla corretta applicazione della normativa europea.

Il Garante per la protezione dei dati personali è l'Autorità amministrativa indipendente incaricata di vigilare sull'applicazione della normativa di protezione dei dati personali, lo scopo è quello di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti fondamentali degli individui. L'Autorità è stata dapprima istituita tramite la legge sulla *privacy* (legge 31 dicembre 1996 n. 675) e trova oggi il proprio fondamento normativo nel D.lgs. n. 196/2003, (Codice *Privacy*), come modificato, in particolare, da *ult*., con il decreto legislativo 10 agosto 2018 n. 101, che designa il Garante come autorità di controllo ai fini dell'attuazione del GDPR[149].

[148] *Ivi*, pp. 155-156.
[149] *Il Garante*, Garante *Privacy*, https://www.garanteprivacy.it/home/autorita.

Sono molteplici gli articoli del GDPR che riguardano la figura dell'Autorità di vigilanza. Nello specifico, l'art. 51 dispone:

> 1. Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«autorità di controllo»).
>
> 2. Ogni autorità di controllo contribuisce alla coerente applicazione del presente regolamento in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione, conformemente al capo VII.
>
> 3. Qualora in uno Stato membro siano istituite più autorità di controllo, detto Stato membro designa l'autorità di controllo che rappresenta tali autorità nel comitato e stabilisce il meccanismo in base al quale le altre autorità si conformano alle norme relative al meccanismo di coerenza di cui all'articolo 63.

In sintesi, lo scopo di questo articolo è quello di stabilire chi controlla che il GDPR venga rispettato e come queste autorità collaborino tra loro, di fatto, le Autorità di controllo dei diversi Paesi UE non lavorano isolate, ma cooperano cercando di applicare il Regolamento nel modo più uniforme, istituendo una disciplina omogena nell'ecosistema dell'Unione.

Il GDPR all'art. 52 designa i poteri delle Autorità:

> 1. Ogni autorità di controllo agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al presente regolamento.
>
> 2. Nell'adempimento dei rispettivi compiti e nell'esercizio dei rispettivi poteri previsti dal presente regolamento, il membro o i membri di ogni autorità di controllo non subiscono pressioni esterne, né dirette, né indirette, e non sollecitano né accettano istruzioni da alcuno.

All'art. 57 si prevede:

1. Fatti salvi gli altri compiti indicati nel presente regolamento, sul proprio territorio ogni autorità di controllo:

> a) sorveglia e assicura l'applicazione del presente regolamento;

b) promuove la consapevolezza e favorisce la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento. Sono oggetto di particolare attenzione le attività destinate specificamente ai minori;

c) fornisce consulenza, a norma del diritto degli Stati membri, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;

d) promuove la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente regolamento;

e) su richiesta, fornisce informazioni all'interessato in merito all'esercizio dei propri diritti derivanti dal presente regolamento e, se del caso, coopera a tal fine con le autorità di controllo di altri Stati membri;

f) tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 80, e svolge le indagini opportune sull'oggetto del reclamo e informa il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole, in particolare ove siano necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo;

g) collabora, anche tramite scambi di informazioni, con le altre autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del presente regolamento;

h) svolge indagini sull'applicazione del presente regolamento, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica;

i) sorveglia gli sviluppi che presentano un interesse, se e in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali;

[…]

k) redige e tiene un elenco in relazione al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4;

[…]

v) svolge qualsiasi altro compito legato alla protezione dei dati personali.

Nello specifico, il ruolo dell'Autorità è di fondamentale rilevanza, soprattutto per quanto concerne il fenomeno del *deepfake*. Si cita a tale proposito la delibera 18 dicembre 2025 che inserisce un avvertimento per gli utilizzatori di servizi di *deepfake*. L'iniziativa si basa su un'attività istruttoria che ha evidenziato la sempre più crescente diffusione dei servizi capaci di generare contenuti artificiali, mediante sistemi di IA. Tali contenuti diffusi, per la maggior parte, attraverso piattaforme *social*, potrebbero essere realizzati e diffusi senza che gli stessi interessati, siano pienamente a conoscenza dell'uso dei propri dati personali nell'ecosistema digitale. Il Garante ha ricordato, citando l'art. 4 paragrafo 1 del GDPR che per "dato personale" deve intendersi qualsiasi informazione riferibile a una persona fisica identificata o identificabile. Seguendo questa prospettiva, sia la voce che l'immagine rappresentano elementi idonei a identificare direttamente un soggetto e, di conseguenza, il loro utilizzo è consentito soltanto nel rispetto dei principi di liceità del trattamento previsti dal GDPR, ossia in presenza di una delle basi giuridiche indicate all'art. 6 del GDPR. Ne consegue che i dati personali inseriti nell'ecosistema digitale possano esporre gli interessati a significati rischi per i propri diritti. Tali rischi, risultano più evidenti nei casi in cui i contenuti artificiali vengono utilizzati con finalità ingannevoli, ad esempio attraverso la creazione di *deepfake* destinati alla sostituzione di persona, contrassegnando situazioni di frodi digitali. L'autorità ha rivolto un avvertimento a tutti i soggetti che utilizzano i sistemi di generazione, evidenziando che il trattamento dei dati, qualora effettuati in assenza di un'idonea base giuridica e senza fornire informazioni chiare e trasparenti, potrebbero determinare la violazione delle norme del GDPR[150].

Di particolare rilievo è il comunicato del 6 maggio 2026 del Garante per la protezione dei dati personali, nel quale l'Autorità ha evidenziato la necessità di disporre di poteri di intervento più incisivi e tempestivi nei confronti delle piattaforme che consentono la creazione e la diffusione di contenuti generativi mediante IA, al fine di contrastare efficacemente la diffusione di *deepfake* e di

[150] *Deepfake: il Garante della Privacy interviene per la tutela dei diritti fondamentali*, IusLetter, 2026, https://iusletter.com/dalla-redazione/intelligenza-artificiale/deepfake-il-garante-della-privacy-interviene-per-la-tutela-dei-diritti-fondamentali/.

altri materiali lesivi dei diritti fondamentali. Comunicato maturata a seguito della circolazione *online* di immagini artificiali raffiguranti il Presidente del Consiglio, Giorgia Meloni, diffusa attraverso diversi canali digitali. Il Garante ha citato espressamente alcune piattaforme come *xAI*, *Grok*, *OpenAI* e *Clothoff*[151]. È la stessa Autorità ad affermare i problemi strutturali: l'oscuramento o il blocco di una determinata piattaforma non elimina il fenomeno, ma anzi, tende a trasferire l'attività verso servizi alternativi. Nel caso specifico, si stima la comparsa di circa 40 nuovi servizi analoghi a *Clothoff* nel periodo del novembre 2025 e aprile 2026. Il blocco attribuisce una misura utile, ma l'intervento avviene normalmente dopo la creazione del contenuto manipolato e quando la diffusione *online* è già iniziata. La diffusone del *deepfake* non è facile da evitare, il tempo per limitare gli effetti è molto breve e spesso bastano poche ore per la diffusine massiva del contenuto. Il Garante, a questo proposito ha evidenziato come l'intervento rapido è essenziale, lo scopo è infatti evitare che la rimozione avvenga troppo tardi e il danno alla persona sia già emerso[152].

3. Tutele civilistiche: profili introduttivi

La giurisprudenza di legittimità ha più volte ribadito che la diffusione dell'immagine è lecita soltanto nei casi previsti dall'art. 97 l. dir. aut. Al di fuori di tali ipotesi, la diffusione dell'immagine, senza il consenso dell'interessato, integra un illecito civile. La Corte di Cassazione, con la sentenza n.11353 del 2010[153], ha affermato che il consenso della persona ritratta rappresenta la regola generale, mentre le deroghe previste dall'art. 97 l. dir. aut., devono essere interpretate restrittivamente. La Corte ha inoltre chiarito che l'interesse pubblico alla conoscenza di una notizia non implica automaticamente anche divulgazione dell'immagine delle persone coinvolte. Come evidenziato dalla Cassazione nella sentenza n. 4477 del 2021[154], la diffusione dell'immagine richiede un bilanciamento tra diritto di cronaca e diritti della personalità della

[151] Quest'ultima, nell'ottobre 2025, era già stata oggetto di un provvedimento di blocco per la generazione di immagini di nudo artificiali realizzate senza il consenso degli interessati.
[152] *Legge 132/2025 e deepfake: il quadro italiano dopo il caso Meloni e le richieste del Garante*, TrueScreen, https://truescreen.io/it/articoli/legge-132-2025-deepfake-quadro-italiano/.
[153] Corte Cass., Sez. III Civile, 11 maggio 2010, n. 11353, consultabile su La Legge per Tutti, https://sentenze.laleggepertutti.it/sentenza/cassazione-civile-n-11353-del-11-05-2010.
[154] Corte Cass., Sez. I Civile, 22 ottobre-19 febbraio 2021, n. 4477.

persona ritratta; la pubblicazione dell'immagine deve risultare essenziale rispetto alla notizia divulgata, non può quindi tradursi in una lesione della dignità e dell'onore della persona[155].

Per quanto riguarda la tutela del diritto all'immagine e la conseguente violazione dello stesso, l'ordinamento prevede diversi rimedi giuridici, che possono essere distinti anche in base al momento in cui intervengono rispetto alla lesione del diritto. In primo luogo, vi è la tutela preventiva, che si realizza attraverso l'azione inibitoria, finalizzata a impedire o interrompere una condotta lesiva, prima che il danno si produca o si aggravi. In secondo luogo, una volta verificata la lesione, trova applicazione la tutela risarcitoria di natura contrattuale o extracontrattuale. Quest'ultima trova fondamento nell'art. 2043 c.c. per quanto concerne il danno patrimoniale e l'art. 2059 c.c. per il danno non patrimoniale.

È in questo contesto che assume una forte centralità la distinzione tra persone note e persone non celebri. Come si è avuto modo di analizzare nel primo capitolo, questa distinzione, non serve solo a capire quando sia accettabile o meno pubblicare la foto di un individuo, ma determina profonde divergenze sul piano risarcitorio, nello specifico, la questione della quantificazione del danno. Nel caso dei soggetti non noti, la lesione del diritto all'immagine si traduce quasi esclusivamente in un danno non patrimoniale, inteso come sofferenza morale e alterazione della vita di relazione. Al contrario, per i soggetti noti, l'immagine possiede un elevato valore economico. Consegue, quindi, che l'abusiva diffusione dell'effige, genera un pregiudizio di natura prevalentemente economica, oltre che non patrimoniale.

Bisogna anche precisare come la tradizionale concezione della responsabilità civile è stata a lungo ricondotta a una funzione esclusivamente compensativa, volta a reintegrare integralmente il patrimonio e la sfera giuridica del soggetto leso mediante il risarcimento del danno subito. Tuttavia, l'evoluzione della giurisprudenza e della dottrina ha progressivamente evidenziato come il

[155] M. CASELLA, *Il c.d. «prezzo del consenso» quale criterio risarcitorio in caso si danno all'immagine*, Njus, 2022, https://www.njus.it/news/2482/il-c-d-prezzo-del-consenso-quale-criterio-risarcitorio-in-caso-di-danno-all-immagine/.

risarcimento possa assolvere anche ulteriori finalità. Accanto alla funzione risarcitoria, infatti, si è progressivamente affermata una funzione preventiva e deterrente, volta a scoraggiare la reiterazione di condotte illecite e a incentivare comportamenti conformi al diritto[156].

In tale prospettiva si colloca il dibattito relativo ai danni punitivi (*punitive damages*), istituto tipico dei sistemi di *common law*, il cui scopo non consiste soltanto nel compensare il danno subito dalla vittima, ma anche nel punire l'autore dell'illecito e nel prevenire la commissione di future condotte analoghe. A differenza del modello tradizionale italiano, fondato sul principio della corrispondenza tra danno risarcibile e pregiudizio effettivamente patito, i *punitive damages* conferiscono al risarcimento una funzione ulteriore rispetto a quella meramente compensativa, introducendo una componente sanzionatoria che trascende la sola reintegrazione del pregiudizio subito.

Per lungo tempo, tale istituto è stato considerato incompatibile con i principi fondamentali dell'ordinamento italiano, in quanto la funzione sanzionatoria era ritenuta prerogativa esclusiva del diritto penale, mentre la responsabilità civile era confinata alla sola riparazione del danno. Tale impostazione ha, tuttavia, subito un significativo ridimensionamento a seguito della sentenza delle Sezioni Unite della Corte di cassazione n. 16601 del 5 luglio 2017[157]. Con tale pronuncia, la Suprema Corte, pur non introducendo i danni punitivi nell'ordinamento interno, ha ammesso la possibilità di riconoscere efficacia alle sentenze straniere che li prevedano, purché non risultino contrari all'ordine pubblico interno[158].

L'aspetto di maggiore rilievo della decisione risiede nell'affermazione secondo cui la responsabilità civile non può più essere ricondotta a una funzione

[156] R. RORDORF, *I "danni punitivi" e la natura polifunzionale della responsabilità civile*, Atlalex, 2023, https://www.altalex.com/documents/2023/08/24/danni-punitivi-natura-polifunzionale-responsabilita-civile.
[157] Corte Cass., Sez. Unite, 5 luglio 2017, n. 16601.
[158] R. RORDORF, *I "danni punitivi" e la natura polifunzionale della responsabilità civile*, Atlalex, 2023, https://www.altalex.com/documents/2023/08/24/danni-punitivi-natura-polifunzionale-responsabilita-civile.

esclusivamente riparatoria, ma presenta una natura polifunzionale, nella quale convivono finalità deterrenti e sanzionatorie[159].

L'affermazione della natura polifunzionale della responsabilità civile assume una particolare rilevanza nel contesto delle nuove tecnologie e degli illeciti digitali. La diffusione di contenuti manipolati mediante sistemi di intelligenza artificiale generativa, infatti, può determinare lesioni estremamente gravi e difficilmente reversibili ai diritti della personalità, rendendo evidente l'esigenza di una tutela che non si limiti alla mera compensazione economica del danno, ma persegua anche finalità preventive e deterrenti.

Tuttavia, la risposta dell'ordinamento non si esaurisce sul piano civilistico. Nei casi in cui la gravità dell'offesa trascenda la dimensione meramente risarcitoria, il legislatore ha ritenuto necessario affiancare alla tutela civile una specifica tutela penale. Il tassello innovativo è rappresentato, dall'art. 612-*quater* c.p. introdotto dalla Legge n. 132/2025. Per la configurazione del reato, il legislatore richiede che il contenuto sia capace di far apparire come autentico un contenuto falso, e che derivi, come conseguenza della condotta lesiva, un danno ingiusto alla reputazione e alla dignità della persona ritratta. Tale fattispecie si coordina strettamente con il reato di *revenge porn* regolato dall'art. 612-*ter* c.p., qualora il *deepfake* presenti una connotazione esplicitamente sessuale (come nel caso dei *deepnude*)[160]. Pur restando al di fuori del perimetro civilistico, il ricorso alla sanzione penale testimonia la presa di coscienza da parte dell'ordinamento nazionale circa la gravità della fattispecie.

L'obiettivo che qui ci si propone è di esaminare le principali tutele civilistiche che l'ordinamento nazionale e comunitario mettono a disposizione per la protezione del diritto all'immagine, al fine di valutarne l'efficacia rispetto al fenomeno del *deepfake*. Essendo una realtà emersa recentemente, la disciplina

[159] S. GANCI, *Nota a Corte di Cassazione – Sezioni Unite Civili, Sentenza 5 luglio 2017 n. 16601*, Ildirittoamministrativo, 2017, https://www.ildirittoamministrativo.it/archivio/allegati/Nota%20a%20Sez%20Un%20Civili%20N%2016601%20del%205%207%2017%20di%20SALVATORE%20GANCI.pdf.

[160] Camera dei deputati, *Introduzione dell'articolo 612-quater del Codice penale, in materia di manipolazione artificiale di immagini di persone reali allo scopo di ottenere rappresentazioni nude*, Scheda di lettura, 2021, https://documenti.camera.it/leg18/dossier/testi/gi0176.htm.

giuridica non appare ancora definita, rendendo necessario il ricorso agli strumenti tradizionali. La crescente esigenza di garantire una protezione effettiva nello spazio digitale, ha inoltre indotto l'Unione europea ad affermare il principio secondo cui le condotte illecite conservano la loro natura anche quando vengono attuate nell'ambiente digitale[161]. In questa prospettiva, la nozione di contenuto illegale nell'ambiente digitale deve essere sostanzialmente coerente con quella già prevista dall'ordinamento per il mondo fisico. Ne consegue che gli utenti delle piattaforme digitali sono tenuti al rispetto dei medesimi obblighi giuridici che gravano sui soggetti operanti *offline* e che, qualora pongano in essere condotte lesive di diritti altrui, trovano applicazioni i tradizionali meccanismi della responsabilità civile, adattati alle peculiarità del contesto tecnologico in cui si realizza la lesione[162].

La finalità che si intende conseguire il presente capitolo non è, pertanto, individuare una tutela destinata a prevalere sulle altre, bensì ricostruire il sistema dei rimedi potenzialmente applicabili per fronteggiare le lesioni del diritto all'immagine derivanti dall'utilizzo dei *deepfake*.

3.1 Tutele preventive: l'azione inibitoria e provvedimenti cautelari

Il panorama digitale ha amplificato la complessità della tutela del diritto all'immagine, soprattutto in relazione al fenomeno del *deepfake*. La creazione e la diffusione di immagini manipolate incidono direttamente sulla violazione dell'identità personale dell'individuo e sulla conseguente percezione sociale.

Nel sistema giuridico italiano la pubblicazione o l'utilizzazione abusiva dell'immagine, al di fuori dei casi espressamente previsti dalla legge, trova una prima tutela nell'art. 10 c.c., che prevede di adire l'autorità giudiziaria per chiedere la cessazione dell'abuso: quest'ultima può ordinare l'immediata

[161] Comunicazione della Commissione, *Illegal and harmful content on the Internet* del 16 ottobre 1996, in C. SOLINAS, *Responsabilità civile e piattaforme digitali*, *I Tematici*, in *Enciclopedia del diritto*, Settimo volume, Giuffrè, 2024, p. 965.
[162] C. SOLINAS, *Responsabilità civile e piattaforme digitali*, *I Tematici*, in *Enciclopedia del diritto*, Settimo volume, Giuffrè, 2024, p. 965.

interruzione dell'abuso e, se ne sussistono i requisiti, la condanna per i responsabili al risarcimento del danno[163].

La salvaguardia delle posizioni giuridiche non può limitarsi ad un intervento riparatorio *ex post*, e quindi una tutela meramente risarcitoria. Risulta invece di rilevante importanza l'adozione di azioni preventive finalizzate a prevenire l'insorgenza di abusi da parte di terzi, minimizzando eventuali lesioni che il fatto illecito possa concretizzare[164].

È l'azione inibitoria che in tali circostanze assume rilievo. Il legislatore non ha fornito una disciplina organica dell'azione inibitoria, ma ne ha predisposto una definizione generale. Un riferimento normativo può risiedere nell'art. 156 l. dir. aut., comma 1[165], che riconosce la possibilità di agire in giudizio.

Accanto all'azione inibitoria, si colloca l'azione risarcitoria, la quale è diretta ad ottenere il risarcimento del danno derivante dalla lesione del diritto. Tramite quest'ultima, infatti, qualora qualcuno abbia utilizzato un'immagine altrui fuori dai casi consentiti dalla legge, il soggetto interessato potrà ottenere il risarcimento del danno derivante da tale uso improprio.

Lo scopo primario dell'inibitoria è quello di imporre la cessazione immediata di un comportamento illecito oppure di impedirne l'attuazione. Tale tutela ha uno scopo duraturo, permanendo per tutta la durata degli effetti della sentenza che lo contiene, fino a un'eventuale modifica della decisione nei successivi gradi di giudizio, o in caso di passaggio ingiudicato in via definitiva. L'elemento che giustifica il ricorso all'azione inibitoria è rappresentato dalla sussistenza di una violazione del diritto tutelato o dal concreto pericolo che essa si verifichi. Diversa

---

[163] G. BAVETTA, *Immagine (diritto alla)*, in *Enciclopedia del diritto*, vol. XX, Giuffrè, Milano, 1970, pp. 153-155.

[164] *Proprietà Intellettuale e mondo digitale | L'importanza di una tutela preventiva*, Dirty Work, 2023, https://www.dirtywork.it/blog/proprieta-intellettuale-e-mondo-digitale-limportanza-di-una-tutela-preventiva/.

[165] «*Chi ha ragione di temere la violazione di un diritto di utilizzazione economica a lui spettante in virtù di questa legge oppure intende impedire la continuazione o la ripetizione di una violazione già avvenuta sia da parte dell'autore della violazione che di un intermediario i cui servizi sono utilizzati per tale violazione può agire in giudizio per ottenere che il suo diritto sia accertato e sia vietato il proseguimento della violazione. Pronunciando l'inibitoria, il giudice può fissare una somma dovuta per ogni violazione o inosservanza successivamente constatata o per ogni ritardo nell'esecuzione del provvedimento*».

è la presenza di un danno e l'accertamento della colpa dell'autore della condotta. La funzione tipica dell'azione inibitoria è preventiva, poiché mira a evitare il verificarsi dell'illecito o a impedire che esso venga reiterato nel tempo: il comportamento da inibire deve quindi presentare una potenzialità lesiva futura[166].

Accanto all'azione inibitoria operano provvedimenti cautelari, ossia misure provvisorie e urgenti che il giudice può adottare per evitare che il tempo necessario alla definizione del giudizio comprometta in modo irreparabile il diritto fatto valere. In tale prospettiva, il ricorso d'urgenza ex art. 700 c.p.c. consente un intervento immediato quando sussistano il *fumus boni iuris*, ossia la ragionevole fondatezza della pretesa, e il *periculum in mora*, consistente nel concreto rischio che l'attesa della decisione di merito provochi un pregiudizio imminente e irreparabile. La funzione di tale rimedio è quindi quella di assicurare una tutela tempestiva, anticipando gli effetti della futura pronuncia di merito nella misura necessaria a evitare che il diritto subisca un danno non più rimediabile[167].

3.2 La responsabilità extracontrattuale: l'art. 2043 c.c.

A seguito della diffusione di contenuti manipolati che ledono il diritto all'immagine, si può configurare un illecito civile.

A questo proposito, si fa riferimento alla responsabilità civile extracontrattuale detta anche "aquiliana", che venne introdotta per prevedere l'obbligo di risarcimento dei danni arrecati ad altri anche in assenza di un rapporto contrattuale tra le parti. Essa, infatti, non trae origine da un vincolo contrattuale e, quindi, da un rapporto preesistente tra danneggiato e danneggiante, ma da un comportamento attivo oppure omissivo della condotta[168].

---

[166] A. PALUMBO, *La tutela inibitoria*, tesi di dottorato, Università degli Studi Roma Tre, 2010, pp 61-64, https://arcadia.sba.uniroma3.it/bitstream/2307/569/1/LA%20TUTELA%20INIBITORIA.pdf.

[167] Cfr. Trib. Milano, Sez. I Civile, ord. 26 gennaio 2026, R.G. n. 1544, Giud. Roberto Pertile, che in accoglimento del ricorso cautelare proposto da Alfonso Signorini, ha ordinato la rimozione immediata dei contenuti lesivi della sua reputazione, immagine e riservatezza, nonché il divieto di ogni ulteriore diffusione. In, M. PANATO, *Deepfake e tutela dell'immagine: i rimedi civili*, Marco Panato studio legale, 2026, https://www.studiolegalemp.info/blog/deepfake-e-tutela-dellimmagine-i-rimedi-civili.html.

[168] AA.VV., *La responsabilità civile*, Milano, IPSOA, 2007, pp. 2-3, https://www.lamiabiblioteca.com/external?url='bookId=11BO0000003932LIBRO.

Storicamente, la responsabilità civile è stata concepita principalmente come uno strumento volto a riparare il pregiudizio subito dal danneggiato mediante risarcimento del danno. Tale funzione riparatoria, tuttavia, non esaurisce il significato dell'istituito. L'evoluzione dell'ordinamento, e in particolare l'influenza dei principi costituzionali, ha progressivamente valorizzato ulteriori funzioni della responsabilità civile, accanto a quella meramente riparatoria[169]. Nel concreto, la giurisprudenza ha utilizzato gli artt. 2, 3 e 32 della Costituzione per rivedere il modo di intendere la responsabilità civile, sia nell'ambito dell'illecito extracontrattuale sia in quello contrattuale.

Per quanto concerne la responsabilità extracontrattuale, essa trova fondamento nell'art. 2043 del Codice civile, al cui interno assumono rilievo tre concetti: il fatto illecito, il danno ingiusto e il risarcimento del danno[170].

3.2.1 Gli elementi oggettivi dell'illecito

Affinché sorga l'obbligo di risarcimento, è necessario che siano presenti determinati presupposti, tradizionalmente distinti in elementi oggettivi ed elementi soggettivi. Gli elementi oggettivi sono inerenti al fatto dannoso e li distinguiamo in: danno ingiusto e nesso di causalità. Gli elementi soggetti riguardano, invece, il soggetto che ha commesso il fatto e comprendono: l'imputabilità e la colpevolezza. Nel corso dell'analisi verranno approfonditi i singoli elementi.

Il primo elemento che verrà analizzato è il danno ingiusto. Il Codice civile non offre una definizione espressa alla nozione di "danno"; tuttavia, il termine compare più volte nell'art. 2043 c.c., la dottrina, ha quindi, evidenziato il carattere polisemico della categoria, precisando come essa assuma differenti significati a seconda della funzione che è chiamata a svolgere[171].

---

[169] E. NAVARRETTA, *Diritti inviolabili e responsabilità civile*, in *Enciclopedia del diritto*, Annali VII, Giuffrè, 2014, p. 343.

[170] A.M. BENEDETTI, *Danno ingiusto: a) profili ricostruttivi generali*, in *Enciclopedia del* diritto, *I Tematici*, Giuffrè, Milano, VII Responsabilità civile, 2024, pp. 372-373.

[171] G. PONZANELLI, *Danni punitivi*, in *Enciclopedia del* diritto, *I Tematici*, Giuffrè, Milano, VII Responsabilità civile, 2024, p. 171.

In passato, prevaleva l'idea che una persona fosse responsabile solo quando violava un divieto normativo volto a ledere il diritto soggettivo specifico. Si è affermata una visione differente: l'illecito ricorre qualora la lesione riguardi un interesse ritenuto dall'ordinamento meritevole di tutela, ponendo al centro dell'indagine non la causa del danno, bensì la tutela del soggetto leso[172]. Quindi, possiamo affermare che il danno è ingiusto quando colpisce una situazione giuridica che il diritto considera meritevole di tutela. Non basta che, la persona lesa subisca una perdita o un pregiudizio, ma è necessario che sussista una lesione di un interesse riconosciuto giuridicamente[173]. A questo proposito, la ricostruzione del concetto di ingiustizia del danno e l'interpretazione dell'art. 2043 c.c. hanno mutato la prospettiva della responsabilità extracontrattuale[174].

Altro elemento oggettivo è il nesso di causalità, a questo proposito bisogna distinguere due diversi momenti valutativi: la causalità di fatto e la causalità giuridica. La prima è volta a verificare il collegamento tra condotta ed evento lesivo, la seconda per la determinazione del danno risarcibile. In ambito civilistico, la semplice lesione dell'interesse tutelato non coincide con il danno risarcibile. La lesione costituisce piuttosto il presupposto dal quale possono derivare conseguenze patrimoniali o non patrimoniali. Per questo motivo, l'accertamento causale si articola in due distinti momenti: il primo volto a stabilire se la condotta abbia determinato l'evento lesivo; il secondo finalizzato a verificare quali effetti dannosi siano effettivamente riconducibili a quell'evento e possano essere oggetto di risarcimento. La causalità materiale individua il fondamento stesso della responsabilità civile, poiché consente di accertare se il danno sia effettivamente conseguenza della condotta del soggetto. In assenza di tale collegamento non può configurarsi alcun illecito civile. La giurisprudenza ha elaborato criteri interpretativi diretti a verificare l'efficienza causale della condotta. Tradizionalmente, trova applicazione il criterio della *conditio sine qua non*, secondo il quale una determinata condotta è causa dell'evento quando

[172] E. NAVARRETTA, *Diritti inviolabili e responsabilità civile*, in *Enciclopedia del diritto*, Annali VII, Giuffrè, 2014, p. 344-345.
[173] A.M. BENEDETTI, *Danno ingiusto: a) profili ricostruttivi generali*, in *Enciclopedia del* diritto, *I Tematici*, Giuffrè, Milano, VII Responsabilità civile, 2024, p. 371.
[174] E. NAVARRETTA, *Diritti inviolabili e responsabilità civile*, in *Enciclopedia del diritto*, Annali VII, Giuffrè, 2014, p. 345.

quest'ultimo non si sarebbe verificato in sua assenza. Tale impostazione, presenta il limite di estendere potenzialmente all'infinito la catena causale, poiché qualsiasi antecedente dell'evento potrebbe essere considerato rilevante. Per superare tale inconveniente, la giurisprudenza ha sviluppato criteri correttivi fondati su una valutazione qualitativa delle circostanze. Si colloca, a tal proposito, la teoria della causalità adeguata, secondo la quale assume rilevanza la condotta che, secondo un giudizio *ex ante* di regolarità causale, appaia idonea a produrre l'evento verificatosi. Accanto alla causalità materiale opera la causalità giuridica, *ex* art. 1223 c.c. e richiamata in materia di responsabilità extracontrattuale (art. 2056 c.c.). Tale disposizione delimita l'ambito del danno risarcibile alle conseguenze che risultino immediate e dirette dell'illecito. Lo scopo di tale istituto è quello di impedire che l'autore dell'illecito risponda di ogni pregiudizio che possa essere collegato all'evento lesivo. Pertanto, è richiesto al giudice, l'individuazione delle conseguenze che facciano sussistere un rapporto sufficientemente stretto con la lesione dell'interesse protetto, escludendo effetti eccezionali o indiretti[175].

3.2.2 Gli elementi soggettivi dell'illecito

L'imputabilità rappresenta uno degli elementi soggettivi dell'illecito civile ed è disciplinato dagli artt. 2046 e 2047 c.c. In base all'art. 2046 c.c. non è responsabile delle conseguenze del fatto illecito chi al momento in cui lo ha commesso era privo di capacità di intendere o di volere. Tuttavia, questa esclusione di responsabilità non sussiste nel momento in cui lo stato di incapacità è stato determinato da un comportamento colposo dello stesso soggetto, come nel caso dell'assunzione volontaria di *alcool* o sostanze stupefacenti. Quando l'illecito è commesso da una persona capace di intendere o di volere, la legge prevede che il risarcimento del danno sussiste a carico di chi era tenuto alla sua sorveglianza, purché dimostri di non aver potuto impedire il fatto.

[175] J. DESTRADI, *Il nesso di causalità quale elemento costitutivo dell'illecito extracontrattuale*, Centro studi Corrado Rossitto, 2024, https://www.centrostudirossitto.it/il-nesso-di-causalita-quale-elemento-costitutivo-dellillecito-extracontrattuale/.

Altro elemento soggettivo è la colpevolezza, che è richiamata dall'art. 2043 cc. Essa si manifesta nelle forme di dolo o colpa[176]. Si ha dolo quando il soggetto pone in essere una condotta con la consapevolezza e la volontà di cagionare l'evento dannoso. In questo caso, il soggetto che ha commesso il fatto è pienamente consapevole delle conseguenze del proprio comportamento e mira deliberatamente a realizzarle.

Si parla di colpa, invece, quando il soggetto agisce contro l'intenzione. L'evento dannoso, pur potendo essere previsto, non è voluto dall'autore, ma si verifica a causa di: negligenza, imprudenza o imperizia. La colpa, pertanto, si caratterizza per la mancanza di volontà nel provocare l'evento, pur essendo riconducibile a un comportamento non diligente o non conforme alle norme di legge.

3.2.3 Il danno risarcibile

La disciplina della responsabilità extracontrattuale distingue il danno patrimoniale, previsto dall'art. 2043 c.c., dal cosiddetto danno non patrimoniale, disciplinato all'art. 2059 c.c. Quest'ultimo si configura su una tutela della sfera personale dell'individuo, comprendendo in modo più ampio la sfera morale e la sofferenza interiore.

Lo scopo della responsabilità civile è quello di assicurare il pieno ristoro del danno, sia patrimoniale che non patrimoniale. In tale prospettiva si afferma il principio della integrale riparazione del pregiudizio, che non trova una tutela costituzionale, ma costituisce uno dei cardini principali all'interno del sistema della responsabilità civile[177].

Le prime problematiche emergono già in riferimento al danno patrimoniale, il quale deve comprendere non solo la perdita subita, ma anche il mancato guadagno

---

[176] Cfr. art. 43 c.p.: «*Il delitto: è doloso, o secondo l'intenzione, quando l'evento dannoso o pericoloso, che è il risultato dell'azione od omissione e da cui la legge fa dipendere l'esistenza del delitto, è dall'agente preveduto e voluto come conseguenza della propria azione od omissione*[(1)]*;*
è preterintenzionale, o oltre l'intenzione, quando dall'azione od omissione deriva un evento dannoso o pericoloso più grave di quello voluto dall'agente;
è colposo, o contro l'intenzione, quando l'evento, anche se preveduto, non è voluto dall'agente e si verifica a causa di negligenza o imprudenza o imperizia, ovvero per inosservanza di leggi, regolamenti, ordini o discipline».

[177] G. PONZANELLI, *Danni punitivi*, in *Enciclopedia del* diritto, *I Tematici*, Giuffrè, Milano, VII Responsabilità civile, 2024, p. 172.

(danno emergente e lucro cessante). Le difficoltà diventano ancora più evidenti per determinare il danno non patrimoniale, poiché la sua valutazione in termini monetari non è caratterizzata da beni o interessi che hanno un immediato valore economico. Proprio la natura di tali interessi rende particolarmente complessa una valutazione pienamente adeguata a determinate il pregiudizio sofferto[178].

L'estensione della tutela del danno non patrimoniale ha infatti comportato il riconoscimento della coesistenza di diversi componenti del pregiudizio come il danno morale, biologico ed esistenziale, pur mantenendo fermo il principio di unitarietà della categoria del danno non patrimoniale e conseguentemente, l'inammissibilità di categoria risarcitorie autonome[179]. Problematica con riguardo ai danni non patrimoniale derivanti dalla lesione dei diritti della personalità, rispetto al mancato parametro di quantificazione oggettivo, sia per l'assenza di precedenti omogenei, sia per la difficoltà di ricorrere a criteri tabellari. Tale situazione, consegue, molto spesso, valutazioni che si traducono in forme di sovracompensazione[180].

Secondo l'impostazione tradizionale, nell'art. 2043 c.c., il dolo e la colpa costituiscono elementi necessari per la configurazione dell'illecito, ma non incidono sulla determinazione quantitativa del danno. Parte della dottrina ha sostenuto che il diverso grado della condotta, valutato in termini di dolo o colpa, dovrebbe riflettersi anche sulla misura concreta del risarcimento. Tale esigenza emerge soprattutto in ambito del risarcimento del danno morale, ambito nel quale il giudice, nell'esercizio del potere equitativo, è chiamato a considerare tutte le circostanze del caso concreto, comprese le condotte dell'autore dell'illecito[181].

A questo proposito, per comprendere in modo più ampio la disciplina del risarcimento e nello specifico del danno patrimoniale e non patrimoniale, bisogna ricordare la distinzione tra soggetti noti e soggetti non noti, nello specifico nel mondo digitale e, soprattutto per l'ambito di studio dell'elaborato, con riferimento

[178] *Ibidem*.
[179] *Ibidem*.
[180] *Ivi*, p. 173.
[181] *Ibidem*.

al fenomeno dei *deepfake*. L'impatto di tali contenuti, infatti, varia sensibilmente a seconda della posizione sociale e mediatica dell'individuo coinvolto.

Nel caso del soggetto non noto, il *deepfake* incide prevalentemente sulla dimensione personale e relazionale. In tale ipotesi, il danno assume natura prevalentemente non patrimoniale, mentre il pregiudizio economico rimane prevalentemente residuale. Diversa è invece la situazione delle persone celebri. È noto, infatti, come lo sfruttamento dell'immagine del soggetto famoso costituisca un rilievo economico. La diffusione non autorizzata dell'immagine di un personaggio noto mediante *deepfake* può sottrarre, in tutto o in parte, la possibilità di sfruttamento economico dell'effige, arrecando un danno per lo più di natura patrimoniale. A ciò si aggiunge l'eventuale lesione dell'onore e della reputazione derivante dalla diffusione di contenuti idonei ad alterare la percezione pubblica della persona.

La liquidazione del danno non patrimoniale derivante dalla lesione dell'onore e della reputazione costituisce uno degli aspetti più complessi all'interno del sistema della responsabilità civile. La difficoltà sta nella valutazione in termini economici della quantificazione del pregiudizio relativo alla dimensione immateriale della persona, e quindi non tanto la condotta lesiva del diritto, ma la conseguente proiezione dell'individuo nel contesto sociale. Il danno non patrimoniale non si configura come una perdita economicamente misurabile, proprio per questo si riconosce la liquidazione equitativa ai sensi dell'art. 1226 c.c.[182]. La giurisprudenza ha progressivamente chiarito che il danno all'onore e alla reputazione non si può considerare "*in re ipsa*" e cioè alla mera verificazione della condotta offensiva, ma deve verificarsi una conseguenza concreta sulla sfera personale del soggetto[183].

L'ampliamento della tutela risarcitoria ha costituito il terreno sul quale si è sviluppata la riflessione circa l'ammissibilità dei danni punitivi, mettendo in discussione il tradizionale principio secondo cui il risarcimento deve limitarsi alla

[182] «*Se il danno non può essere provato nel suo preciso ammontare, è liquidato dal giudice con valutazione equitativa*».
[183] M. ROSSETTI, *Danno non patrimoniale: c) profili della liquidazione*, in *Enciclopedia del* diritto, *I Tematici*, Giuffrè, Milano, VII Responsabilità civile, 2024, pp. 550-551.

sola reintegrazione del pregiudizio subito. Ciò che può assumere una funzione punitiva, non è tanto la componente sanzionatoria che viene a collocarsi sul piano dell'evento dannoso, bensì rispetto alla risposta risarcitoria predisposta dall'ordinamento[184]. In una prospettiva generale, il danno punitivo può essere inteso come una particolare forma di tutela risarcitoria che attribuisce al soggetto leso una somma eccedente la mera reintegrazione del pregiudizio subito. Si tratta di un meccanismo che opera a favore del danneggiato[185].

Il diritto italiano degli ultimi decenni ha mostrato una crescente apertura a modelli di responsabilità civile caratterizzati da funzioni non solo riparatorie, ma anche preventive e deterrenti. Rimane però, la difficoltà di stabilire una base normativa sufficientemente solida per fondare una vera e propria categoria di danni punitivi. Parte della dottrina ha individuato nell'art. 1226 c.c. uno degli strumenti che consentono al giudice una valutazione equitativa del danno; tuttavia, tale disposizione non costituisce una base normativa autonoma per l'attribuzione di una funzione punitiva al risarcimento[186]. La giurisprudenza ha più volte affrontato il tema del danno punitivo soprattutto riguardo al dibattito relativo alla distinzione tra danno-evento e danno-conseguenza, il primo di matrice penalistica che si riferisce alla lesione dell'interesse e il secondo riguarda gli effetti pregiudizievoli concretamente subiti dal danneggiato e risarcibile ai sensi dell'art. 1223 c.c. Il danno-evento individua una lesione dell'interesse giuridicamente protetto e costituisce il presupposto per l'accertamento della responsabilità. È qui che subentra il cosiddetto danno *in re ipsa*, concetto che non deve essere confuso con il danno punitivo, quest'ultimo svolge, infatti, una funzione differente: non mira a compensare il pregiudizio subito, ma a sanzionare la condotta del responsabile particolarmente riprovevole mediante risarcimento eccedente la mera reintegrazione del danno[187].

Nel primo capitolo è stata richiamata la sentenza della Corte di Cassazione n. 1557 del 5 aprile 1978, fondamentale per comprendere l'evoluzione del criterio

[184] G. PONZANELLI, *Danni punitivi*, in *Enciclopedia del* diritto, *I Tematici*, Giuffrè, Milano, VII Responsabilità civile, 2024, p. 171.
[185] *Ivi*, p. 172.
[186] *Ivi*, p. 173.
[187] *Ivi*, p. 175.

quantitativo del danno risarcibile. L'analisi storica della giurisprudenza assume un ruolo essenziale che consente di evidenziare come la disciplina del risarcimento del danno sia caratterizzata da una continua trasformazione interpretativa. La sentenza del 1978 rappresenta uno dei primi tentativi della giurisprudenza di ampliare la tutela della persona, superando la primaria concezione patrimoniale del danno, riconoscendo una tutela alla lesione della sfera personale del soggetto leso[188].

A tale proposito, è importante citare la pronuncia della Corte di Cassazione del 31 maggio 2003[189], che ha proposto un'interpretazione dell'art. 2059 c.c. maggiormente orientata alla tutela dei valori costituzionali della persona. Infatti, il danno non patrimoniale non coincide esclusivamente con il danno morale tradizionalmente inteso, ma ricomprende ogni lesione di interessi inerenti alla persona, pur privi di immediata rilevanza economica. Fondata primariamente su una tutela che ha alla base la centralità della persona. Il danno morale concerne il turbamento emotivo e la sofferenza psichica provocati dall'evento dannoso; il danno biologico, invece, consiste nella lesione dell'integrità psicofisica della persona e richiede un accertamento fondato su criteri medico-legali. Accanto a tali figure, si colloca il c.d. danno esistenziale, forma di pregiudizio che si configura quando il fatto illecito altera concretamente il modo di vivere della vittima, incidendo nel concreto sulle abitudini di vita quotidiana del soggetto leso[190].

Per comprendere, ancora meglio, l'evoluzione del risarcimento del danno non patrimoniale, può essere citata la sentenza della Corte di Cassazione n. 26972 del 2008, dove la Corte ha posto fine a un lungo dibattito giurisprudenziale relativo alla configurabilità del cosiddetto "danno esistenziale", quale categoria autonoma rispetto al danno non patrimoniale. La Corte ha chiarito come non possano essere riconosciute sottocategorie di danno non patrimoniale, poiché una simile frammentazione renderebbe eccessivamente atipico il sistema risarcitorio, con il

[188] Corte Cass., Sez. I Civile, 5 aprile 1978, n. 1557, massima pubblicata su *Avvocato.it,* https://www.avvocato.it/massimario-36717/.
[189] Corte Cass., Sez. III Civile, 31 maggio 2003, n. 8828.
[190] M. IASELLI, *Danno esistenziale, configurabilità e liquidazione: la Cassazione fa il punto*, Atlalex, 2013, https://www.altalex.com/documents/news/2013/08/28/danno-esistenziale-configurabilita-e-liquidazione-la-cassazione-fa-il-punto.

rischio di ampliare indiscriminatamente le ipotesi di risarcimento oltre i limiti previsti dall'ordinamento. In tale prospettiva, l'art. 2059 del c.c. è stato interpretato come norma già idonea e sufficiente a garantire una tutela piena ed effettiva del danno non patrimoniale, purché la lesione riguardi diritti inviolabili della persona costituzionalmente garantiti[191].

Per quando riguarda la liquidazione equitativa è interessante sviluppare l'evoluzione della giurisprudenza in merito. La Corte di Cassazione ha dichiarato più volte che la pubblicazione non autorizzata dell'immagine di una persona può determinare non solo un danno non patrimoniale, ma anche conseguenze economiche pregiudizievoli. La giurisprudenza di legittimità ha riconosciuto al soggetto danneggiato la possibilità di ottenere il risarcimento del danno per via di un pregiudizio economico derivante dall'utilizzo abusivo della propria immagine quando si riesca a fornire prova delle perdite subite e del mancato guadagno. La tutela risarcitoria può comunque sussistere mediante il ricorso al criterio equitativo del "prezzo del consenso", che consente di determinare il danno facendo riferimento alla somma presumibile che il titolare del diritto avrebbe richiesto per autorizzare la pubblicazione della propria immagine, garantendo una liquidazione proporzionata ed equa alla luce dei criteri presenti all'art. 158 comma 2 l. dir. aut. La Cassazione con sentenza n. 12433 del 2008 ha evidenziato come risulti complesso quantificare il danno economico, soprattutto quando la persona ritratta non gode di notorietà tale da attribuire alla propria effige un valore commerciale determinabile[192].

Un passaggio decisivo sul piano evolutivo si è avuto con la sentenza della Corte di Cassazione n. 26973 dell'11 novembre 2008, ridefinendo in maniera sistematica la categoria del danno patrimoniale. Fu in questa sede che venne elaborata la distinzione, precedentemente accennata, tra il danno-evento dal danno-conseguenza: il primo coincide con la lesione del diritto protetto, il secondo riguarda gli effetti concreti che derivano dalla lesione del diritto. La Corte ha

[191] Corte Cass., Sez. Unite, n. 26972/2008, in Federalismi.it, https://www.federalismi.it/nv14/articolo-documento.cfm?artid=11303.
[192] M. CASELLA, *Il c.d. «prezzo del consenso» quale criterio risarcitorio in caso si danno all'immagine*, Njus, 2022, https://www.njus.it/news/2482/il-c-d-prezzo-del-consenso-quale-criterio-risarcitorio-in-caso-di-danno-all-immagine/.

esplicitato come la mera violazione del diritto non fa sussistere un danno risarcibile, ma richiede la prova delle conseguenze effettivamente subite. Cambiando così, la quantificazione del danno, in base alla valutazione concreta delle ripercussioni prodotte dall'illecito[193].

La responsabilità extracontrattuale, quindi, costituisce il rimedio successivo rispetto alla tutela inibitoria, consentendo il ristoro delle conseguenze patrimoniali e non patrimoniali.

3.3 Diritto all'oblio: l'art. 17 GDPR

L'art 17 del GDPR rubricato "*Diritto alla cancellazione - Diritto all'oblio*" dispone:

> *1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:*
>
> *a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;*
>
> *b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;*
>
> *c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;*
>
> *d) i dati personali sono stati trattati illecitamente;*
>
> *e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; ([1])*
>
> *f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.*
>
> *[...]*

[193] Corte Cass., Sez. Unite, 11 novembre 2008, n. 26973.

3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; ([1])

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

La diffusione di *Internet* ha trasformato profondamente il significato del diritto all'oblio. In passato, la circolazione delle informazioni personali era legata principalmente ai mezzi di comunicazioni tradizionali, come giornali e pubblicazioni cartacee; la distribuzione risultava limitata nel tempo e nello spazio. Oggi, la realtà digitale rende complesso il controllo dei dati personali una volta immessi nella rete. L'aspetto più problematico non è di per sé, la rimozione del contenuto originario pubblicato, quanto la presenza della diffusione di copie condivise e riprodotte da soggetti diversi, continuando ad essere accessibili anche dopo la loro cancellazione dalla fonte iniziale, per via della diffusione attraverso i molteplici canali *online*. Il diritto all'oblio richiede una riflessione sulla permanenza delle informazioni nel *web*. La questione centrale riguarda la possibilità che dati e contenuti che continuano a essere reperibili anche quando hanno perso ogni rilevanza da parte dell'interesse pubblico. La facilità con cui le informazioni digitali vengono conservate e replicate rende, infatti, difficile il loro effettivo superamento nel tempo. La sfida della società contemporanea non consiste più nel preservare la memoria dell'informazione, ma nel riuscire a

limitare la persistenza, garantendo la possibilità di essere dimenticati quando non sussistano più ragioni di interesse pubblico che ne giustifichino la diffusione[194].

Il diritto alla cancellazione dei dati personali trova il fondamento giuridico all'art. 17 del GDPR. L'esercizio del diritto da parte dall'interessato non costituisce una condizione necessaria affinché i dati vengano eliminati, quando si verifica una delle circostanze previste dalla norma, il titolare del trattamento è tenuto ad attivarsi autonomamente per procedere alla cancellazione dei dati, senza attendere una richiesta esplicita da parte dell'interessato. Quest'ultimo può presentare domanda formale di cancellazione qualora ritenga che i propri dati siano ancora tratti in assenza di presupposti di legge. In tali casi la richiesta può avvenire con modalità libere, salvo che il titolare abbia predisposto specifiche procedure per l'esercizio dei diritti riconosciuti dal Regolamento. Una volta ricevuta l'istanza o accertata la sussistenza delle condizioni previste dall'art. 17 del GDPR, il titolare deve intervenire tempestivamente[195].

Il Considerato 59 del GDPR sottolinea l'obbligo di predisporre strumenti che facilitino l'esercizio dei diritti degli interessati. Risulta, quindi, opportuno il coinvolgimento di personale competente chiamato a verificare l'esistenza dei presupposti per la cancellazione. Conclusa l'analisi del caso, il titolare deve comunicare all'interessato l'esito della valutazione. Qualora il diritto alla cancellazione non risulti applicabile, occorre fornire una motivazione adeguata del diniego. Se sussistono le condizioni richieste, devono essere avviate le operazioni necessarie per eliminare i dati e informare l'interessato dell'avvenuta cancellazione. Un ulteriore obbligo riguarda la comunicazione della cancellazione a tutti i soggetti ai quali i dati erano stati precedentemente trasmessi, inclusi responsabili e contitolari del trattamento. Tale adempimento può essere omesso solo nei casi in cui risulti impossibile o comporti uno sforzo manifestamente sproporzionato[196].

---

[194] A. CATALETA, *Diritto all'oblio e privacy, cos'è e come esercitarlo: tutto quello che devi sapere*, Agenda Digitale, 2025, https://www.agendadigitale.eu/sicurezza/privacy/il-diritto-alloblio/.
[195] *Ibidem*.
[196] *Ibidem*.

Il diritto alla cancellazione non ha carattere assoluto. L'art. 17, paragrafo 3 del GDPR, individua alcune situazione nelle quali il titolare può continuare a conservare i dati personali nonostante la richiesta dell'interessato. Ciò avviene quando un obbligo normativo impone la conservazione dei dati per un determinato periodo di tempo. La conservazione può risultare necessaria nel consentire l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. In tali circostanze l'interesse alla tutela giurisdizionale prevale sulla richiesta di cancellazione, consentendo all'organizzatore di mantenere i dati per il tempo strettamente necessario alla salvaguardia delle proprie ragioni[197].

Nonostante il GDPR abbia definito le modalità e i limiti dell'esercizio del diritto di cancellazione dei dati personali, la sua effettiva applicazione continua a presentare numerose criticità derivate, sia sulla necessità di conciliare tale diritto con gli altri interessi giuridicamente tutelati, sia dalle caratteristiche dell'ambiente digitale che, spesso, rendono complessa l'attuazione concreta della disposizione normativa. La persistente capacità delle tecnologie digitali di conservare, replicare e diffondere informazioni su scala globale pone importanti interrogativa circa l'effettività del diritto all'oblio. Le informazioni, una volta diffuse *online*, tendono a permanere attraverso copie e ripubblicazione che sfuggono al controllo diretto dell'interessato[198].

4. La responsabilità delle piattaforme digitali e l'art. 82 GDPR

Fenomeni come i *deepfake* evidenziano come il danno possa derivare da processi tecnologici complessi, nei quali l'individuazione del soggetto materialmente autore dell'illecito risulta particolarmente problematica.

È proprio in situazioni di questo tipo che assume rilievo la categoria della responsabilità oggettiva, la quale consente di prescindere in tutto o in parte dall'accertamento della colpa del soggetto chiamato a rispondere. Occorre tuttavia precisare che la responsabilità oggettiva non costituisce una categoria unitaria. La dottrina distingue tradizionalmente diverse forme di responsabilità oggettiva.

[197] *Ibidem*.
[198] *Ibidem*.

Una prima figura è rappresentata dalla responsabilità oggettiva pura, nella quale il soggetto risponde del danno indipendentemente dall'accertamento della colpa, essendo sufficiente il verificarsi dell'evento dannoso riconducibile alla situazione di rischio posta a suo carico. In tali ipotesi, l'imputazione del danno prescinde integralmente da qualsiasi valutazione della condotta diligente del responsabile, il quale non può liberarsi dimostrando di aver adottato tutte le cautele possibili. Nella responsabilità oggettiva il danneggiato deve provare il danno, il nesso di causalità tra il fatto e il pregiudizio subito. Non è invece tenuto a dimostrare la colpa del responsabile.

Accanto ad essa si collocano le forme di responsabilità oggettiva aggravata nelle quali permane la possibilità di andare esenti da responsabilità attraverso la prova di specifiche circostanze liberatorie. In questi casi la responsabilità continua a fondarsi su un criterio oggettivo di imputazione del rischio, ma non assume carattere assoluto, essendo temperata dalla possibilità di dimostrare l'esistenza di fattori idonei ad escludere la responsabilità. In quest'ultima opera un'inversione dell'onere della prova: una volta che il danneggiato abbia provato il danno, il nesso causale e i presupposti della fattispecie, spetta al convenuto fornire la prova liberatoria per andare esente da responsabilità.

Questa distinzione assume particolare importanza nell'ambito della tutela dei dati personali e, più in generale, della responsabilità derivante dall'utilizzo di sistemi di intelligenza artificiale. Come si vedrà nell'analisi dell'art. 82 del GDPR, il legislatore europeo non ha configurato una forma di responsabilità oggettiva pura del titolare o del responsabile del trattamento. La disciplina, infatti, pur perseguendo un elevato livello di protezione dell'interessato e agevolando il risarcimento del danno, prevede una causa di esonero da responsabilità qualora il titolare o il responsabile dimostrino che l'evento dannoso non è in alcun modo imputabile alla propria sfera di controllo.

L'analisi di tale disciplina risulta particolarmente significativa con riferimento ai *deepfake*. In queste ipotesi, infatti, il danno può derivare non soltanto dalla condotta dell'autore materiale della manipolazione, ma anche dall'attività di ulteriori soggetti che intervengono nella filiera tecnologica, quali le piattaforme

che diffondono il contenuto, i fornitori dei servizi di intelligenza artificiale o altri operatori coinvolti nel trattamento dei dati personali.

L'art. 82 GDPR rubricato "*Diritto al risarcimento e responsabilità*" stabilisce quanto segue:

> *1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.*
>
> *2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.*
>
> *3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.*

L'art. 82 GDPR prevede che: il titolare dei dati deve adottare misure tecniche ed organizzative adeguate a prevenire i rischi derivanti dal trattamento dei dati. Se si verifica un danno, il titolare deve dimostrare di aver adottato tutte le misure necessarie per evitarlo; in caso contrario sarà responsabile del danno cagionato.

La responsabilità civile sorge qualora l'interessato provi la sussistenza di un danno concreto, sia patrimoniale che non patrimoniale, e il relativo nesso di causalità con la condotta illecita. Sebbene l'articolo 82, paragrafo 3, esoneri il titolare solo in caso di totale assenza di imputabilità dell'evento dannoso, l'orientamento interpretativo prevalente esclude la configurabilità di una responsabilità oggettiva pura. In combinazione con le misure di prevenzione previste, la fattispecie si qualifica propriamente come un'ipotesi di colpa presunta, il cui elemento caratterizzante è l'inversione dell'onere della prova. Non spetta, quindi, al

danneggiato dimostrare il comportamento negligente, bensì, spetta al titolare dare dimostrazione l'eventuale adeguatezza delle misure adottate[199].

La responsabilità da illecito trattamento dei dati affronta un profilo problematico che riguarda, non tanto la configurazione del danno, ma il relativo regime probatorio e la funzione che il risarcimento del danno non patrimoniale è chiamato a svolgere nel sistema delineato dal GDPR. La difficoltà che caratterizzano l'accertamento della prova del danno immateriale che, non può essere compresa appieno senza interrogarsi sulla finalità della tutela risarcitoria prevista dall'art. 82 del Regolamento. Sul punto, la Corte di Giustizia ha chiarito che il diritto al risarcimento, riconosciuto da tale disposizione, è finalizzato a garantire l'integrale ristoro del pregiudizio sopportato dal soggetto leso, escludendo qualsisia attribuzione di natura punitiva[200]. Sebbene l'art. 82 GDPR si collochi all'interno di un sistema che comprende anche gli artt. 83 e 84 GDPR, destinati a disciplinare il regime sanzionatorio delle violazioni, la funzione repressiva e deterrente è affidata esclusivamente a tali strumenti, mentre la responsabilità prevista all'art. 82 GDPR conserva una vocazione primariamente compensativa. La giurisprudenza europea traccia una linea di confine per quanto concerne la nozione di danno immateriale. Il risarcimento, infatti, deve essere commisurato al pregiudizio concretamente sofferto dal soggetto leso. L'art. 82 GDPR rappresenta uno strumento fondamentale di tutela del diritto alla protezione dei dati personali. Attraverso il risarcimento del danno, il GDPR, garantisce una protezione effettiva dell'interessato e rafforza il rispetto delle regole sul trattamento dei dati da parte dei titolari[201].

Per comprendere, ancora più nel dettaglio, il rapporto tra responsabilità civile e piattaforme digitali, bisogna precisare il significato attribuito all'espressione "piattaforme digitali". In una prima prospettiva la piattaforma è considerata come un soggetto cui possono essere imputati obblighi, doveri e responsabilità. In una

[199] A. FUSARO, *La responsabilità civile europea da illecito trattamento dei dati personali: le ricadute di diritto interno*, in *Nuova giur. civ. comm*., 2026, II, in corso di pubblicazione.
[200] CGUE, 4 maggio 2023, C-300/21, in A. FUSARO, *La responsabilità civile europea da illecito trattamento dei dati personali: le ricadute di diritto interno*, in *Nuova giur. civ. comm*., 2026, II, in corso di pubblicazione.
[201] *Ibidem*.

seconda terminologia essa viene intesa come spazio virtuale nel quale gli individui svolgono attività di varia natura, come l'instaurazione di relazioni sociali e l'accesso a informazioni. Vi è un'altra definizione di carattere tecnico-giuridico, secondo la quale la piattaforma costituisce un servizio su richiesta di un destinatario, da un prestatore che consente la memorizzazione e la diffusione di contenuti destinati al pubblico come sancito dall'art. 3, lettera i), del DSA[202].

In tale quadro si colloca il tema della responsabilità civile delle piattaforme digitali intese come soggetti che erogano il servizio, per gli illeciti commessi dagli utenti nell'ambiente digitale. Come già specificato, le piattaforme svolgono un servizio di intermediazione essenziale, in quanto consentono la circolazione dei flussi informativi che caratterizzano l'attività digitale degli utenti, e nello specifico la funzione delle piattaforme si sostanzia nella memorizzazione dei contenuti e nella loro successiva diffusione al pubblico. In merito al ruolo di intermediazione si è posto il problema se nasca un rapporto causale indiretto che possa trasformarsi in una responsabilità giuridica in capo al prestato del servizio per gli illeciti commessi dagli utilizzatori della piattaforma[203]. A tale proposito, alle piattaforme è richiesto di collaborare al contrasto di contenuti illeciti presenti in rete, nonché di evitare che *Internet* venga utilizzato come strumento per la commissione di illeciti[204].

L'art 54 del DSA prevede che il fornitore del servizio sia tenuto a risarcire il danno subito dal destinatario qualora la violazione di uno degli obblighi stabiliti dal Regolamento abbia causato un pregiudizio. Ne consegue che, anche l'adozione di misure di contrasto non fondate possano arrecare un danno all'utente della piattaforma, giustificando l'introduzione di una regola uniforme che ne assicuri il diritto al risarcimento. Nell'ordinamento italiano, tale previsione si colloca nella disciplina della responsabilità contrattuale, derivante dagli adempimenti degli obblighi che il prestatore assume nei confronti dell'utente. Per quanto riguarda la responsabilità verso terzi in relazione alla diffusione di

[202] C. SOLINAS, *Responsabilità civile e piattaforme digitali*, in *Enciclopedia del* diritto, *I Tematici*, Giuffrè, Milano, VII Responsabilità civile, 2024, p. 964.
[203] *Ibidem*.
[204] *Ivi*, p. 966.

contenuti caricati dagli utenti, il DSA conferma l'impianto delle esenzioni "orizzontali" previsto dalla Direttiva 2000/31/CE[205]. Nello specifico, l'art. 6 stabilisce che il prestatore dei servizi di *hosting*, categoria nella quale rientrano anche le piattaforme *online*, non è responsabile dei contenuti memorizzati quando non sia a conoscenza dell'effettiva illiceità delle informazioni, né, sia consapevole dei fatti o circostanze che rendono evidenti la loro natura illecita. In alternativa, l'esenzione opera anche se, una volta acquisita tale conoscenza, il prestatore interviene tempestivamente per rimuovere i contenuti o disabilitarne l'accesso. Infine, l'art. 16, paragrafo 3, del DSA specifica che la conoscenza effettiva o la consapevolezza dell'illecito possono essere acquisite anche tramite segnalazioni conformi ai requisiti del Regolamento, purché tali comunicazioni siano sufficientemente precise da consentire a un prestatore di individuare il contenuto illecito senza necessità di un'analisi giuridica approfondita [206].

Lo scopo del Regolamento è quello di definire un perimetro di esonero o di limitazione della loro esposizione giuridica rispetto ai contenuti illeciti generati e immessi *online* degli utenti. In altri termini, l'intervento si concentra sulla delimitazione negativa delle condizioni in cui l'intermediario non può essere chiamato a rispondere più che sulla configurazione positiva di specifiche fattispecie di responsabilità civile. Le conseguenze tipiche della responsabilità civile e in particolare l'obbligazione risarcitoria ex art. 2043 c.c., rimangono sullo sfondo e continuano a trovare la loro disciplina principale nel sistema nazionale. Il DSA non sostituisce tali regole, ma si limita a incidere sulla loro operatività. Il capo II del DSA può essere letto come *safe harbour*, entro il quale determinati prestatori di servizi non sono esposti automaticamente a conseguenze giuridiche per le attività illecite poste in essere dagli utenti, non limitando la possibilità di una responsabilità, ma ne condiziona l'insorgenza al verificarsi di specifici

[205] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»).
[206] *Ivi*, pp. 981-982.

presupposti normativi, riducenti l'area di rischio giuridico connessi alla mera funzione tecnica di intermediazione[207].

Il DSA conferma nel considerando n.17 come le disposizioni del Regolamento operino in parallelo alle norme nazionali ed europee in materia di responsabilità civile, senza sostituirle o assorbirle. Le norme contenute al Capo II del DSA non delineano un regime generale di responsabilità civile degli intermediari, ma piuttosto un insieme di condizioni e limiti che coordinano l'operatività delle regole già esistenti nei diversi ordinamenti. Resta ferma la scelta di modelli di imputazione dei danni di tipo oggettivo, cioè svincolati dall'accertamento di un comportamento colposo o comunque da presupposti di conoscenza e interventi dell'intermediario. Tale opzione riflette l'intento di evitare che il ruolo meramente tecnico e neutrale delle piattaforme si traduca automaticamente in una forma di responsabilità piena per i contenuti veicolati dagli utenti, preservando così un equilibrio tra tutela dei diritti e sviluppo dei servizi digitali [208].

4.1 La Direttiva (UE) 2024/2853 sulla responsabilità del produttore per danno da prodotto difettoso

L'intervento normativo europeo si è reso necessario al fine di adeguare il quadro giuridico tradizionale alle profonde trasformazioni tecnologiche che hanno caratterizzato gli ultimi decenni. In particolare, la crescente diffusione di *software*, prodotti digitali e sistemi di intelligenza artificiale, evidenziato i limiti di una disciplina concepita in un contesto economico completamente diverso da quello attuale.

In questo scenario assume particolare rilievo il ruolo del legislatore europeo. Con la Direttiva (UE) 2024/2853 (*Product Liability Directive*, LPD)[209], il legislatore europeo ha avviato un profondo aggiornamento della disciplina della responsabilità per danno da prodotti difettosi. La nuova normativa sostituirà, a partire dal 9 dicembre 2026, la storica Direttiva 85/374/CE[210], che per quasi

[207] *Ibidem*.
[208] *Ivi*, pp. 983-984.
[209] Pubblicazione della Direttiva nella Gazzetta Ufficiale dell'Unione europea il 18 novembre 2024.
[210] Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi.

quarant'anni ha rappresentato il principale riferimento in materia di tutela dei consumatori nei confronti dei danni causati da prodotti difettosi[211]. Uno degli aspetti più innovativi riguarda l'ampliamento della nozione di prodotto. Accanto ai beni materiali tradizionali, vengono ora inclusi anche i *software*[212].Tale scelta consente di ricomprendere chiaramente, nell'ambito applicativo della normativa, anche i sistemi basati sull'intelligenza artificiale, garantendo ai consumatori una tutela effettiva nei confronti dei danni eventualmente causati da tali tecnologie. La direttiva conferma il principio della responsabilità oggettiva del produttore. In questa prospettiva, il produttore di *software* o il fornitore di sistemi di intelligenza artificiale viene considerato responsabile al pari del produttore tradizionalmente inteso[213]. La normativa introduce importanti agevolazioni probatorie per i soggetti danneggiati. Tradizionalmente, chi agiva per ottenere il risarcimento doveva dimostrare l'esistenza del difetto, il danno subito e il nesso causale tra i due elementi. Nel caso delle tecnologie particolarmente complesse, come i sistemi di intelligenza artificiale, tale dimostrazione può risultare estremamente difficile. Per questo motivo la direttiva prevede specifiche presunzioni che facilitano la prova della responsabilità, riducendo l'onere gravante sul consumatore[214][215].

[211] La disciplina relativa alla responsabilità per danno da prodotto difettoso, nell'ordinamento italiano, trova fondamento agli artt. 114-127 del Codice del Consumo (D.lgs 6 settembre 2005, n. 206). Nello specifico l'art. 114 del Codice del Consumo sancisce il principio secondo cui il produttore è responsabile del danno cagionato dai difetti del prodotto da lui immesso sul mercato. La responsabilità si fonda su un criterio di natura oggettiva, in quanto il soggetto danneggiato non è tenuto a dimostrare la colpa del produttore, ma soltanto l'esistenza del danno, il difetto del prodotto e il nesso causale tra i due elementi.

[212] Cfr. art. 4 PLD: «*1) «prodotto»: ogni bene mobile, anche se integrato in un altro bene mobile o in un bene immobile o interconnesso con questi; include l'elettricità, i file per la fabbricazione digitale, le materie prime e il software; 2) «file per la fabbricazione digitale»: una versione digitale di un bene mobile o un modello digitale per un bene mobile contenente le istruzioni funzionali necessarie per produrre un bene tangibile consentendo il controllo automatizzato di macchine o strumenti*».

[213] Cfr. art. 4, paragrafo 10), PLD: «*10) «fabbricante»: qualsiasi persona fisica o giuridica che: a) sviluppa, produce o fabbrica un prodotto; b) fa progettare o fabbricare un prodotto o che, apponendo il proprio nome, marchio o altre caratteristiche distintive su tale prodotto, si presenta come fabbricante; o c) sviluppa, produce o fabbrica un prodotto per uso proprio*».

[214] Cfr. art. 10 PLD: «*2. Si presume il carattere difettoso di un prodotto qualora sia soddisfatta una delle seguenti condizioni: a) il convenuto omette di divulgare i pertinenti elementi di prova a norma dell'articolo 9, paragrafo 1; b) l'attore dimostra che il prodotto non rispetta i requisiti obbligatori di sicurezza del prodotto stabiliti dal diritto dell'Unione o nazionale intesi a proteggere dal rischio del danno subito dal danneggiato; o c) l'attore dimostra che il danno è stato causato da un malfunzionamento evidente del prodotto durante l'uso ragionevolmente prevedibile o in circostanze ordinarie. 3. Si presume l'esistenza del nesso di causalità tra il carattere difettoso del*

4.2 Regimi speciali di responsabilità: la responsabilità per l'esercizio di attività pericolose

Tra le disposizioni del Codice civile che potrebbero trovare applicazione rispetto ai danni causati dall'intelligenza artificiale, un ruolo particolarmente rilevante è svolto dall'art. 2050 c.c., che disciplina la responsabilità per l'esercizio di attività pericolose. Tale norma prevede che:

> *Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.*

L'applicazione di questa disciplina ai sistemi di intelligenza artificiale dipende in primo luogo dalla possibilità di qualificare il loro utilizzo come "attività pericolosa". Sul punto la dottrina ha evidenziato come la nozione di attività pericolosa non sia definita in modo tassativo, richiedendo una valutazione caso per caso, fondata sulla natura dell'attività o sulla caratteristica dei mezzi utilizzati. Sono considerate pericolose non solo le attività espressamente qualificate come tali dalla legge, ma anche quelle che presentano una probabilità di arrecare danni per la loro potenzialità offensiva[216]. La responsabilità prevista dall'art. 2050 c.c. si fonda sull'accertamento del nesso causale tra l'attività svolta e l'evento dannoso. Una volta che il danneggiato abbia dimostrato il collegamento causale tra l'attività e il pregiudizio subito, grava sull'esercente l'onere di provare di aver adottato tutte le misure idonee ad evitare il danno. La natura di tale responsabilità è oggetto di un ampio dibattito. Secondo un orientamento dottrinale, essa configura una responsabilità aggravata fondata su una presunzione di colpa, in quanto la prova

---

prodotto e il danno nel caso in cui sia stato provato che il prodotto è difettoso e che la natura del danno cagionato è compatibile con il difetto in questione. 4. L'organo giurisdizionale nazionale presume il carattere difettoso del prodotto o il nesso di causalità tra il carattere difettoso e il danno, o entrambi, qualora, nonostante la divulgazione di prove a norma dell'articolo 9 e tenuto conto di tutte le circostanze pertinenti del caso: a) l'attore incontri difficoltà eccessive, in particolare a causa della complessità tecnica o scientifica, nel provare il carattere difettoso del prodotto o il nesso di causalità tra il carattere difettoso e il danno o entrambi; e b) l'attore dimostri che è probabile che il prodotto sia difettoso o che esista un nesso di causalità tra il carattere difettoso del prodotto e il danno, o entrambi».

[215] S. M. CUCCIARRÈ, S. D. CASCONE, G. F. BONACCI, *La nuova Product Liability Directive e le novità in materia di IA*, Rodl, 2024, https://www.roedl.it/it/temi/legal-newsletter/11-2024/nuova-product-liability-directive-novita-materia-ia.

[216] V. Corte Cass, Sez. III Civile, 20 maggio 2015, n. 10268, in L. DI DONNA, *Intelligenza artificiale e rimedi risarcitori*, CEDAM, 2022, p. 131.

liberatoria è incentrata sulla dimostrazione della diligenza adottata. Parte della giurisprudenza, invece, la qualifica come una forma di responsabilità oggettiva o, quantomeno, caratterizzata da criteri di imputazione oggettivi, poiché l'accertamento della responsabilità prescinde dalla colpa in senso soggettivo e si incentra sulla pericolosità dell'attività e sul nesso causale con l'evento dannoso[217].

L'applicazione dell'art. 2050 c.c. ai sistemi di intelligenza artificiale richiede di distinguere tra l'utilizzo dell'IA in astratto e il suo impegno concreto. Se, infatti, il semplice ricorso all'intelligenza artificiale non può essere considerato automaticamente un'attività pericolosa, vi sono casi in cui il suo utilizzo può rendere pericolosa un'attività che, in assenza di tale tecnologia, non presenterebbe tale qualificazione. Ciò può accadere, ad esempio, nei settori della produzione industriale e dell'attività medica, sempre più caratterizzati dall'impiego di sistemi autonomi in grado di incidere direttamente su interessi giuridici particolarmente rilevanti, quali salute e sicurezza della persona. In tale prospettiva, parte della dottrina ritiene che, i sistemi di intelligenza artificiale ad alto rischio possano rientrare nell'ambito applicativo dell'art. 2050 c.c., soprattutto quando caratterizzati da elevati livelli di autonomia decisionale e capacità di autoapprendimento[218]. A sostengo di questa tesi sono stati richiamati alcuni precedenti giurisprudenziale relativi alla commercializzazione dei prodotti da fumo, qualificata come attività pericolosa[219]. Secondo tale orientamento, se la produzione di sigarette è stata considerata pericolosa per gli elevati rischi che comporta la salute umana, analogamente potrebbe essere qualifica come pericolosa la produzione di sistemi di intelligenza artificiale dotati di autonomia e imprevedibilità operativa. Ne consegue che la disciplina della responsabilità per attività pericolose potrebbe trovare applicazione in via alternativa, rispetto alla responsabilità del produttore. L'orientamento maggioritario ammette infatti la

[217] *Ivi*, p. 121-128.
[218] *Ivi*, pp. 134-135.
[219] Corte Cass., Sez. III Civile, 17 dicembre 2009, n. 26516, in L. DI DONNA, *Intelligenza artificiale e rimedi risarcitori*, CEDAM, 2022, pp. 134-135.

cumulabilità dei due regimi quando il danno sia causato da un prodotto che risulti difettoso e pericoloso[220].

[220] *Ibidem*.

CONCLUSIONE

Tra la fine del Novecento e l'inizio del nuovo millennio, le visioni utopiche ottimistiche vengono progressivamente sostituite da scenari sempre più pessimistici. Questi cambiamenti sono spesso collegati al venire meno della fiducia nel progresso e nell'idea che lo sviluppo dell'umanità conduca inevitabilmente verso un futuro migliore, convinzione che aveva caratterizzato gran parte del secolo precedente. Tuttavia, il timore per ciò che ci attende non coincide con un rifiuto del futuro, sebbene siano sempre più evidenti i rischi legati all'innovazione tecnologica, emerge la consapevolezza che tale processo non possa essere fermato, ma non viene più recepito esclusivamente come fonte benefica[221].

Particolarmente rilevante rispetto all'attuale società dell'informazione è l'inserimento dell'individuo nel flusso continuo di dati. In questo contesto, non è più sufficiente limitarsi a proteggere ciò che deve rimanere privato, ma diventa necessario garantire all'utente un controllo consapevole sui propri dati personali e sulle modalità del loro utilizzo. La protezione dei dati personali supera la dimensione tradizionale della riservatezza, coinvolgendo aspetti della vita essenziali. Questa evoluzione incide profondamente sui rapporti tra cittadini e istituzioni, tra consumatori e imprese e, più in generale, tra gli individui stessi. Se da un lato tali cambiamenti offrono opportunità di sviluppo, dall'altro possono favorire la nascita di società caratterizzate da sorveglianza e classificazione degli individui[222].

L'analisi sviluppata nel presente elaborato consente di evidenziare come il diritto all'immagine rappresenti, oggi, uno dei diritti della personalità maggiormente esposto alle trasformazioni determinate dall'evoluzione tecnologica e dalla diffusione di sistemi di intelligenza artificiale generative.

Nel primo capitolo è stato ricostruito il percorso storico, normativo e giurisprudenziale che ha condotto all'affermazione del diritto all'immagine quale diritto fondamentale della persona. L'analisi dell'ordinamento nazionale, della

[221] S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, Bologna, 2021, p. 43.
[222] *Ivi*, p. 100.

dimensione comunitaria e del sistema convenzionale della CEDU ha mostrato come la protezione dell'effige non si circoscriva alle mere disposizioni normative interne, ma si interseca in un sistema multilivello di tutela. La giurisprudenza ha svolto un ruolo centrale nell'adattare, alle categorie giuridiche tradizionali, le nuove esigenze sociali, ampliando il concetto d'immagine fino a ricomprendervi ogni elemento idoneo a identificare e rappresentare l'individuo nella società.

Il secondo capitolo ha evidenziato come la rivoluzione digitale abbia profondamente trasformato le modalità di raccolta, elaborazione e circolazione dei dati personali. In tale contesto, la profilazione assume un ruolo centrale, poiché consente di raccogliere e organizzare ingenti quantità di informazioni relative agli individui, creando patrimoni informativi che rappresentano una risorsa essenziale per l'addestramento dei sistemi di intelligenza artificiale. Quanto più ampio, dettagliato e diversificato è il patrimonio di dati utilizzato, tanto maggiore è la capacità degli algoritmi di apprendere caratteristiche fisiche, espressive e comportamentali delle persone. È proprio su tale base che si sviluppa il fenomeno dei *deepfake* che costituisce una delle manifestazioni più significative dell'evoluzione dell'intelligenza artificiale generativa e rappresenta il principale oggetto di indagine del presente lavoro. L'analisi si è quindi soffermata sulle diverse tipologie di *deepfake* e sui principali ambiti applicativi, evidenziando anche come tali strumenti possano essere impiegati per finalità pregiudizievoli per i diritti della persona, quali il *deepnude* e la diffusione di *fake news*. Inoltre, tale ricostruzione ha evidenziato come la crescente disponibilità di dati personali reperibili nell'ambiente digitale abbia determinato un'evoluzione qualitativa dei *deepfake*, rendendoli strumenti capaci di riprodurre l'identità visiva di una persona con un livello di fedeltà tale da rendere sempre più complessa la distinzione tra contenuto autentico e contenuto artificiale. Questo dimostrando come la lesione non derivi più soltanto dalla diffusione non autorizzata dell'immagine, ma anche dalla sua manipolazione artificiale, idonea ad alterare la percezione della realtà e a compromettere l'identità personale del soggetto rappresentato.

Alla luce di tali criticità, il terzo capitolo si è posto l'obiettivo di analizzare gli strumenti di tutela predisposti dall'ordinamento giuridico nazionale e

comunitario. Dall'esame delle recenti iniziative europee, quali il DSA e l'*AI Act*, emerge la volontà da parte del legislatore europeo di stabilire un sistema preventivo di gestione dei rischi derivanti dalle piattaforme digitali e dai sistemi di intelligenza artificiale. Parallelamente, il ruolo del Garante per la protezione dei dati personali si conferma centrale nell'attività di vigilanza e controllo sul trattamento dei dati e sulla protezione dei diritti fondamentali.

Sul piano civilistico, gli strumenti tradizionali quali: l'azione inibitoria, i provvedimenti cautelari, il risarcimento del danno e la responsabilità per l'esercizio di attività pericolose, insieme agli strumenti emersi in ambito comunitario rispetto alla tutela dei dati personali, incluso l'esercizio del diritto all'oblio, e nell'ambito della disciplina consumeristica in particolare riguardo alla responsabilità del produttore per i danni da prodotto difettoso, continuano a rappresentare importanti forme di tutela, pur evidenziando alcune difficoltà di fronte alla diffusione dei contenuti digitali.

In tale contesto appare opportuno valorizzare maggiormente i rimedi riconducibili alla tutela preventiva, i quali, risultano particolarmente idonei a fronteggiare le peculiarità dei contenuti sintetici generati mediante l'intelligenza artificiale. Tale tutela presenta il vantaggio di incidere sulla circolazione del contenuto manipolato, offrendo una protezione che va oltre la mera compensazione economica del danno. Anche i meccanismi di segnalazione e rimozione dei contenuti *online* introdotti dal DSA possono contribuire in modo significativo a mitigare le conseguenze derivanti dalla diffusione di immagini o video alterati, riducendone la circolazione e contenendone l'impatto lesivo sulla sfera personale dei soggetti coinvolti.

Tuttavia, l'effettività di tali meccanismi incontra rilevanti criticità nella pratica, in particolare, nel contesto digitale, la rapidità di diffusione dei contenuti rendono complesso garantire interventi tempestivi ed efficaci, con il rischio che la rimozione o la limitazione della diffusione intervengano quando la lesione si è già ampiamente prodotta e diffusa.

Il diritto all'immagine, nato come tutela della rappresentazione fisica dell'individuo, ha progressivamente ampliato il proprio ambito applicativo sino a diventare una componente essenziale della più ampia tutela dell'identità personale e della dignità umana. Ad oggi, questo diritto, si conferma uno dei principali sistemi di confronto tra progresso tecnologico e tutela della persona. La sfida per il legislatore, la giurisprudenza e le autorità di controllo sarà quella di elaborare strumenti sempre più efficaci per garantire che la potenzialità offerte dall'intelligenza artificiale possano svilupparsi senza compromettere i diritti fondamentali dell'individuo.

In questo quadro di tensione tra innovazione tecnologica e tutela dei diritti fondamentali, assume particolare rilievo il ruolo dell'interprete. Si può affermare, quindi, che la giurisprudenza assume un ruolo centrale non solo quale soggetto chiamato ad applicare le norme, ma soprattutto come interprete dinamico del diritto, capace di adattare la normativa alle esigenze concrete del caso e all'evoluzione della realtà sociale e tecnologica, come dimostrato dall'evoluzione giurisprudenziale in materia di diritto all'immagine e dalla progressiva elaborazione dei criteri di liquidazione. Non solo, la giurisprudenza interviene attraverso l'utilizzo e la rimodulazione dei rimedi già esistenti, adattandoli alle nuove forme di lesione dei diritti. In tal modo, i rimedi tradizionali vengono reinterpretati e resi funzionali a fattispecie nuove.

Tale funzione adattiva dell'interprete, tuttavia, si inserisce in un contesto sempre più complesso, in cui il rapporto tra diritto e innovazione tecnologica mette in evidenza i limiti strutturali degli strumenti giuridici tradizionali. L'attuale scenario fa, però, emergere problemi sul rapporto tra diritto e tecnologia, la crescente complessità delle innovazioni ha infatti evidenziato i limiti del diritto sul fronte dei progressi. Tradizionalmente il diritto ha cercato di mantenere la propria autonomia attraverso il principio del "*iudex peritus peritorum*", secondo cui il giudice conserva la decisione finale, senza delegare integralmente tale funzione

agli esperti; tuttavia, la complessità delle questioni rende più difficile affidarsi esclusivamente a tale impostazione[223].

[223] *Ivi*, p. 142.

BIBLIOGRAFIA

AA.VV., *La responsabilità civile*, Milano, IPSOA, 2007, https://www.lamiabiblioteca.com/external?url='bookId=11BO0000003932LIBRO

ALPA G., RESTA G., *Le persone fisiche e i diritti della personalità*, UTET Giuridica, 2006.

AZZALI V., ELLECOSTA N., *La questione deepfake in Italia: una panoramica*, *MediaLaws*, *Rivista di Diritto dei Media*, 2024.

AZZARITI G., *Stefano Rodotà e l'uso costituzionalmente orientato delle nuove tecnologie*, in Costituzionalismo.it, n.2, Editoriale Scientifica, 2022.

BARBUTO F. M., *Adesso una piattaforma online permette di smascherare i deepfake*, E-Campus Blog, 2024 https://blog.uniecampus.it/2024/10/01/deepfake-o-meter-un-programma-per-smascherare-i-deepfake/ (consultato il 05/05/2026).

BASSETTI N., *GAN (Generative Adversarial Networks): cosa sono, applicazioni e vantaggi*, Agenda Digitale, 2023, https://www.agendadigitale.eu/cultura-digitale/gan-generative-adversarial-networks-cosa-sono-applicazioni-e-vantaggi/ (consultato il 05/05/2026).

BAVETTA G., *Immagine (diritto alla)*, in *Enciclopedia del diritto*, vol. XX, Giuffrè, Milano, 1970.

BENEDETTI A. M., *Danno ingiusto: a) profili ricostruttivi generali*, in *Enciclopedia del* diritto, *I Tematici*, Giuffrè, Milano, VII Responsabilità civile, 2024.

BERGMANN D., *Cos'è il machine learning?*, IBM, 2025, https://www.ibm.com/it-it/think/topics/machinelearning#:~:text=Il%20machine%20learning%20%C3%A8%20il%20sottoinsieme%20dell'AI,per%20fare%20inferenze%20accurate%20sui%20nuovi%20dati (consultato il 03/05/2026).

BOGDANOVIC M., *Il diritto alla tutela dell'immagine personale. Disciplina, problematiche e modello di liberatoria*, Altalex, 2020, https://www.altalex.com/documents/news/2020/10/29/diritto-tutela-immagine-personale (consultato il 16/03/2026).

BUTCHER M., *The startup behind that deep-fake David Beckham video just raised $3M*, TechCrunch, 2019, https://techcrunch.com/2019/04/25/the-startup-

behind-that-deep-fake-david-beckham-video-just-raised-3m/ (consultato il 07/05/2026).
CALDERINI B., *Digital Services Act: cos'è e cosa prevede la legge europea sui servizi digitali*, Agenda Digitale, aggiornato nel 2025, https://www.agendadigitale.eu/mercati-digitali/digital-services-act-cose-e-cosa-prevede-la-legge-europea-sui-servizi-digitali/ (consultato il 15/05/2026).
CASELLA M., *Il c.d. «prezzo del consenso» quale criterio risarcitorio in caso si danno all'immagine*, Njus, 2022, https://www.njus.it/news/2482/il-c-d-prezzo-del-consenso-quale-criterio-risarcitorio-in-caso-di-danno-all-immagine/ (consultato il 28/05/2026).
CASTROREALE R., *Profilazione e Big Data: risvolti su privacy e sicurezza*, InSic, 2024, https://www.insic.it/privacy-e-sicurezza/information-security/profilazione-e-big-data-risvolti-su-privacy-e-sicurezza/. (consultato il 24/04/2026).
CATALETA A., *Diritto all'oblio e privacy, cos'è e come esercitarlo: tutto quello che devi sapere*, Agenda Digitale, 2025, https://www.agendadigitale.eu/sicurezza/privacy/il-diritto-alloblio/ (consultato il 27/05/2026).
CAVARERO A., *Il populismo digitale. L'illusione della democrazia diretta*, Rai Cultura, 2019, https://www.raicultura.it/filosofia/articoli/2019/01/Adriana-Cavarero-il-populismo-digitale-d2149873-58ed-442d-88a5-21bc90ac7aeb.html (consultato il 18/04/2026).
CHIZZOLA E., *DEEPFAKE: tra furto d'identità, danno d'immagine e rischio privacy*, in Norme&Tributi Plus Diritto, Il Sole24Ore, 2021, https://ntplusdiritto.ilsole24ore.com/art/deepfake-furto-d-identita-danno-d-immagine-e-rischio-privacy-AE9Bowf (consultato il 04/05/2026).
CIRILLO A., *Il nuovo reato: il Deepfake*, Studio Cataldi, il diritto quotidiano, 2026, https://www.studiocataldi.it/articoli/48017-il-nuovo-reato-il-deepfake.asp (consultato il 04/05/2026).
COLOMBO R., *Ma li avete letti i nuovi termini d'uso di CapCut?*, Fotografi Digitali, 2025, https://www.fotografidigitali.it/news/ma-li-avete-letti-i-nuovi-termini-d-uso-di-capcut_140252.html (consultato il 07/05/2026).

CONTISSA G., GALLI F., *La governance della "disinformazione aumentata" tra Digital Services Act e AI Act*, Federalismi, n. 15, 2025.
CUCCIARRÈ S. M., CASCONE S. D., BONACCI G. F., *La nuova Product Liability Directive e le novità in materia di IA*, Rodl, 2024, https://www.roedl.it/it/temi/legal-newsletter/11-2024/nuova-product-liability-directive-novita-materia-ia (consultato il 16/06/2026).
DEIBEL T., *The Civil Law and the Inner Self: Roman Iniuria and the Transformation of the Private Sphere*, *Journal of Civil Law Studies*, 16, n. 1, 2024.
DEL RE C., *Tutela del diritto all'immagine: nozione estensiva del Tribunale di Milano,* nota a sentenza su *Tribunale di Milano*, *21 gennaio 2014,* pubblicata in *Il diritto industriale*, n. 3, 2015.
DELLA PIAZZA S., *Il caso Cambridge Analytica*, DirittoConsenso, 2021, https://www.dirittoconsenso.it/2021/12/21/il-caso-cambridge-analytica/ (consultato il 18/04/2026).
DELLI PONTI A., *Le immagini nel web: come usarle in modo legalmente corretto*, Studio Legale Delli Ponti, 2025, https://www.studiolegaledelliponti.eu/le-immagini-nel-web-come-usarle-in-modo-legalmente-corretto/#Immagini_e_fotografie_dal_web (consultato il 07/05/2026).
DESTRADI J., *Il nesso di causalità quale elemento costitutivo dell'illecito extracontrattuale*, Centro studi Corrado Rossitto, 2024, https://www.centrostudirossitto.it/il-nesso-di-causalita-quale-elemento-costitutivo-dellillecito-extracontrattuale/ (consultato il 12/06/2026).
DI DONNA L., *Intelligenza artificiale e rimedi risarcitori*, CEDAM, 2022.
FERRARA L., *Il diritto sulla propria immagine nel nuovo Codice civile e nella nuova legge sul diritto d'autore, Edizioni italiane,* Roma, 1942.
FINOCCHIARO G., *Identità personale (diritto alla)*, in *Digesto delle discipline privatistiche*, UTET, Torino, 2010.
FLINDERS M., SUSNJARA S., SMALLEY I., *Che cos'è un'unità di elaborazione grafica (GPU)?*, IBM, 2025, https://www.ibm.com/it-it/think/topics/gpu (consultato il 03/05/2026).
FUMAGALLI A., *Web scraping: cos'è, perché si usa e come difendersi da*

"intrusioni" indesiderate, Agenda Digitale, 2025, https://www.agendadigitale.eu/sicurezza/web-scraping-cose-perche-si-usa-e-come-difendersi-da-intrusioni-indesiderate/ (consultato il 28/04/2026).

GALLO P., *Intelligenza artificiale e protezione dei dati personali*, in *Digesto delle discipline privatistiche*, UTET, Torino, 2024 (aggiornato nel 2025).

GANCI S., *Nota a Corte di Cassazione – Sezioni Unite Civili, Sentenza 5 luglio 2017 n. 16601*, Ildirittoamministrativo, 2017, https://www.ildirittoamministrativo.it/archivio/allegati/Nota%20a%20Sez%20Un%20Civili%20N%2016601%20del%205%207%2017%20di%20SALVATORE%20GANCI.pdf (consultato il 20/06/2026).

HOLDSWORTH J., *Che cos'è il bias AI?*, IBM, https://www.ibm.com/it-it/think/topics/ai-bias (consultato il 24/04/2026).

IASELLI M., *Danno esistenziale, configurabilità e liquidazione: la Cassazione fa il punto*, Atlalex, 2013, https://www.altalex.com/documents/news/2013/08/28/danno-esistenziale-configurabilita-e-liquidazione-la-cassazione-fa-il-punto (consultato il 12/06/2026).

LAVECCHIA V., *Differenza tra deep learning e rete neurale*, Informatica e Ingegneria *Online*, 2021, https://vitolavecchia.altervista.org/differenza-tra-deep-learning-e-rete-neurale/ (consultato il 05/05/2026).

MIGLIETTI L., *Profili storico-comparativi del diritto alla privacy*, Diritti Comparati, 2014, https://www.dirittocomparati.it/profili-storico-comparativi-del-diritto-alla-privacy/ (consultato il 10/05/2026).

NAVARRETTA E., *Diritti inviolabili e responsabilità civile*, in *Enciclopedia del diritto*, Annali VII, Giuffrè, 2014.

ORLANDO A., *La regolamentazione del deepfake in Europa, Stati Uniti e Cina*, *MediaLaws, Rivista di diritto dei media,* 2025, https://www.medialaws.eu/wp-content/uploads/2025/02/I-24-Orlando.pdf.

PALUMBO A., *La tutela inibitoria*, tesi di dottorato, Università degli Studi Roma Tre, 2010, https://arcadia.sba.uniroma3.it/bitstream/2307/569/1/LA%20TUTELA%20INIBITORIA.pdf (consultato il 27/05/2026).

PANATO M., *Deepfake e tutela dell'immagine: i rimedi civili*, Marco Panato studio legale, 2026, https://www.studiolegalemp.info/blog/deepfake-e-tutela-dellimmagine-i-rimedi-civili.html (consultato il 22/06/2026).
PERON S., *Il nuovo perimetro di liceità per la pubblicazione di immagini di un atleta senza il suo consenso*, *MediaLaws, Rivista di diritto dei media*, 2023, https://www.medialaws.eu/il-nuovo-perimetro-di-liceita-per-la-pubblicazione-di-immagini-di-un-atleta-senza-il-suo-consenso/ (consultato il 18/03/2026).
PINO G., *L'identità personale*, in S. RODOTÀ, M. TALACCHINI (a cura di), *Trattato di biodiritto*, vol. I, Giuffrè, Milano, 2010.
PONZANELLI G., *Danni punitivi*, in *Enciclopedia del* diritto, *I Tematici*, Giuffrè, Milano, VII Responsabilità civile, 2024.
RODOTÀ S., *Tecnologie e diritti*, Il Mulino, Bologna, 2021.
RORDORF R., *I "danni punitivi" e la natura polifunzionale della responsabilità civile*, Atlalex, 2023, https://www.altalex.com/documents/2023/08/24/danni-punitivi-natura-polifunzionale-responsabilita-civile (consultato il 20/06/2026).
ROSSETTI M., *Danno non patrimoniale: c) profili della liquidazione*, in *Enciclopedia del* diritto, *I Tematici*, Giuffrè, Milano, VII Responsabilità civile, 2024.
RUGGIU D., *Dalla profilazione al controllo: come ci manipola l'IA applicata alla politica*, Agenda Digitale, 2026, https://www.agendadigitale.eu/cultura-digitale/dalla-profilazione-al-controllo-come-ci-manipola-lia-applicata-alla-politica/ (consultato il 18/04/2026).
SAGLIMBENI S., *Privacy e tutela dell'immagine della persona: cosa dice la legge*, Agenda Digitale, 2021, https://www.agendadigitale.eu/sicurezza/privacy/privacy-e-tutela-dellimmagine-della-persona-cosa-dice-la-legge/ (consultato l'11/03/2026).
SCALINI A., *Il diritto alla riservatezza*, Giuffrè, Milano, 2002.
SOLINAS C., *Responsabilità civile e piattaforme digitali*, in *Enciclopedia del* diritto, *I Tematici*, Giuffrè, Milano, VII Responsabilità civile, 2024.
STEFANELLI S., *AI Act e responsabilità penale: cosa cambia per provider e deployer*, Agenda Digitale, 2024, https://www.agendadigitale.eu/sicurezza/privacy/ai-act-e-responsabilita-penale-

cosa-cambia-per-provider-e-deployer/#:~:text=Il%20deployer%20%C3%A8%20invece%20la,'attivit%C3%A0%20personale%20non%20professionale%E2%80%9D (consultato il 02/06/2026).

SYNODINOU T., *Image Right and Copyright Law in Europe: Divergences and Convergences*, in *Laws*, vol. 3, n. 2, 2014.

THOBANI S., *Diritti della personalità e contratto: dalle fattispecie tradizionali al trattamento in massa dei dati personali*, Ledizioni, Milano, 2018.

TOLOSANA R., ROMEO-TAPIADOR S., FIERREZ J., VERA-RODRIGUEZ R., *Deepfakes Evolution: Analysis of Facial Regions and Fake Detection Performance*, arXiv, 2020, https://arxiv.org/abs/2004.07532, (consultato il 05/05/2026).

URCIUOLI M. A., *Autonomia negoziale e diritto all'immagine*, Edizioni scientifiche italiane, 2000.

WARREN S., BRANDEIS D., L. D., *The Right to Privacy*, in *Harvard Law Review*, vol. 4, n. 5, 1890.

SITOGRAFIA

CapCut Terms of Service, ultimo aggiornamento 15 aprile 2026, https://www.capcut.com/clause/terms-of-service (consultato il 07/05/2026).

Che cos'è Grok: la nuova AI creata da Elon Musk, Young Platform Academy, 2025, https://academy.youngplatform.com/tecnologia/che-cos-e-grok-la-nuova-ai-creata-da-elon-musk/ (consultato il 21/05/2026).

Che cos'è il footprint digitale? E come proteggerlo dagli hacker, Kaspersky, https://www.kaspersky.it/resource-center/definitions/what-is-a-digital-footprint (consultato il 24/04/2026).

Comprendere i diversi tipi di attacchi generativi AI Deepfake, iProov, 2023, https://www.iproov.com/it/blog/generative-ai-attack-types-explained/ (consultato il 07/05/2026).

Deepfake: il Garante della Privacy interviene per la tutela dei diritti fondamentali, IusLetter, 2026, https://iusletter.com/dalla-redazione/intelligenza-artificiale/deepfake-il-garante-della-privacy-interviene-per-la-tutela-dei-diritti-fondamentali/ (consultato il 25/05/2026).

Dipartimento per le Politiche Europee. *Carta dei diritti fondamentali dell'Unione europea*. https://www.affarieuropei.gov.it/it/normativa/diritti-fondamentali/carta-dei-diritti-fondamentali-dellue/ (consultato il 5/03/2026).

È illecita la diffusione di foto di un minore senza il consenso di uno dei genitori?, Lexet, 2024. https://lexet.it/e-illecita-la-diffusione-di-foto-di-un-minore-senza-il-consenso-di-uno-dei-genitori/ (consultato il 18/03/2026).

AI per Open Source Datasets: Dati per l'Addestramento, in Culture Digitali, https://culturedigitali.eu/notizie/ai-per-open-source-datasets-dati-per-laddestramento/ (consultato il 28/04/2026).

Camera dei deputati*, Introduzione dell'articolo 612-quater del Codice penale, in materia di manipolazione artificiale di immagini di persone reali allo scopo di ottenere rappresentazioni nude*, Scheda di lettura, 2021, https://documenti.camera.it/leg18/dossier/testi/gi0176.htm (consultato il 04/05/2026).

Entra in vigore il regolamento sull'IA, COMMISSIONE EUROPEA, 2024, https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-

01_it (consultato il 19/05/2026).
Garante per la protezione dei dati personali, *Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali*. *Assenza di sistemi per la verifica dei minori*, Garante Privacy, 2023, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847 (consultato il 07/05/2026).
Garante per la protezione dei dati personali, *Deepfake: dal Garante una scheda informativa sui rischi dell'uso malevolo di questa tecnologia*, 2020, Deepfake: dal Garante una scheda informativa sui rischi dell'uso... - Garante Privacy (consultato il 04/05/2026).
Il diritto d'autore delle immagini pubblicate su Internet e sui social media, Studio Corradini, 2025, https://www.corradini.it/il-diritto-dautore-delle-immagini-pubblicate-su-internet-e-sui-social-media/ (consultato il 07/05/2026).
Il Garante, Garante Privacy, https://www.garanteprivacy.it/home/autorita (consultato il 24/05/2026).
In *Navigazione della legge sull'IA*, EU Digital Strategy, 2026, https://digital-strategy.ec.europa.eu/it/faqs/navigating-ai-act (consultato l'11/06/2026).
L'agghiacciante report Meter sulla pedopornografia: oltre 8mila vittime di deepnude. Dagli 8 ai 12 anni i più colpiti, Pro vita & Famiglia, 2026, https://www.provitaefamiglia.it/blog/lagghiacciante-report-meter-sulla-pedopornografia-oltre-8mila-vittime-di-deepnude-dagli-8-ai-12-anni-i-piu-colpiti# (consultato il 04/05/2026).
Legge 132/2025 e deepfake: il quadro italiano dopo il caso Meloni e le richieste del Garante, TrueScreen, https://truescreen.io/it/articoli/legge-132-2025-deepfake-quadro-italiano/ (consultato il 25/05/2026).
La Commissione infligge ammende per un importo di 120 milioni di EUR a norma della legge sui servizi digitali, Shaping Europe's digital future, 2025, https://digital-strategy.ec.europa.eu/it/news/commission-fines-x-eu120-million-under-digital-services-act (consultato l'11/06/2026).
Legge sui servizi digitali: Domande e risposte, Shaping Europe's digital future, 2025, https://digital-strategy.ec.europa.eu/it/faqs/digital-services-act-questions-and-answers (consultato il 02/06/2026).

Polizia Postale, *Come riconoscere un deepfake*, Commissariato di PS *Online*, 2024, https://www.commissariatodips.it/notizie/articolo/come-riconoscere-un-deepfake/index.html (consultato il 05/05/2026).

Proprietà Intellettuale e mondo digitale| L'importanza di una tutela preventiva, Dirty Work, 2023, https://www.dirtywork.it/blog/proprieta-intellettuale-e-mondo-digitale-limportanza-di-una-tutela-preventiva/ (consultato il 26/05/2026).

RIFERIMENTI GIURISPRUDENZIALI

CGUE, 14 febbraio 2019, C-345/17.

CGUE, 24 settembre 2019, C-136/17.

CGUE, 4 maggio 2023, C-300/21.

CEDU, *Von Hannover c. Germania*, 24 giugno 2004, n. 59320/00.

CEDU, *Sciacca c. Italia*, 11 gennaio 2005, n. 50774/99.

CEDU, *Reklos e Davourlis c. Grecia*, 15 gennaio 2009, n. 1234/05.

CEDU, *Couderc e Hachette Filipacchi Associés c. Francia*, 10 novembre 2015, n. 40454/07.

Corte Cost., 7 aprile 1988, n. 404.

Corte Cost., 3 febbraio 1994, n. 13.

Corte Cass., Sez. I Civile, 5 aprile 1978, n. 1557, massima pubblicata su *Avvocato.it,* https://www.avvocato.it/massimario-36717/.

Corte Cass., Sez. I Civile, 16 aprile 1991, n. 4031, in *Diritto dell'Informazione e dell'Informatica*, 1991.

Corte Cass., Sez. III Civile, 31 maggio 2003, n. 8828.

Corte Cass., Sez. Unite, 11 novembre 2008, n. 26972, in Federalismi.it, https://www.federalismi.it/nv14/articolo-documento.cfm?artid=11303.

Corte Cass., Sez. Unite, 11 novembre 2008, n. 26973.

Corte Cass., Sez. III Civile, 17 dicembre 2009, n. 26516.

Corte Cass., Sez. III Civile, 11 maggio 2010, n. 11353, consultabile su La Legge per Tutti, https://sentenze.laleggepertutti.it/sentenza/cassazione-civile-n-11353-del-11-05-2010.

Corte Cass, Sez. III Civile, 20 maggio 2015, n. 10268.

Corte Cass, Sez. Unite, 5 luglio 2017, n. 16601.

Corte Cass., Sez. I Civile, 22 ottobre-19 febbraio 2021, n. 4477.

Trib. Milano, 27 febbraio 1969, in A. SCALINI, *Il diritto alla riservatezza*, Giuffrè, Milano, 2002, p. 73.

Trib. Milano, Sez. I Civile, ord. 26 gennaio 2026, R.G. n. 1544.

Cour de cassation, 1ère ch. civ., 20 mars 2007, n. 06-10.305.