Lezione I
LIBERTÀ, DOVEROSITÀ, INTERNET

Sommario: 1. Frammentazione e metamorfosi delle categorie di tempo e spazio. – **2.** Le trasformazioni delle fonti del diritto nella dimensione digitale. Un'introduzione. – **2.1.** La regolazione attraverso *soft law* e *fast law*. – **2.2.** La Dichiarazione dei diritti su Internet come primo tentativo di ridefinire l'ambito oggettivo dei diritti fondamentali. – **3.** Piattaforme digitali e diritti fondamentali. Un'introduzione. – **4.** Nuovi fenomeni on line. – **4.1.** Il cyberbullismo. – **4.2.** Il *revenge porn*. – **4.3.** Il *deepfake*. – **5.** Prospettive distopiche e neocostituzionalismo digitale.

1. Frammentazione e metamorfosi delle categorie di tempo e spazio

Il tempo in cui viviamo è segnato da cambiamenti profondi che sfidano le capacità di adattamento della società, in generale, e del fenomeno giuridico, in particolare, all'interno del nuovo contesto tecnologico.

Con specifico riferimento all'ambito soggettivo e a quello oggettivo delle libertà personali è sempre più evidente uno sforzo di sovrapposizione di nuove modalità regolatorie rispetto a quelle tradizionali, data l'esigenza di assicurare una forma di riconoscimento e tutela ai nuovi diritti emersi nella realtà digitale. Se, agli albori della rete, si tendeva a riconoscere un'estensione delle categorie giuridiche tradizionali per il godimento dei diritti nello spazio virtuale, oggi questa prospettiva è stata progressivamente superata. Si è formato nel tempo un nuovo quadro di principi e valori connesso all'evoluzione dei rapporti sociali, alle nuove tecniche di informazione, all'espansione dei media, alla costante moltiplicazione di tecnologie informatiche e digitali.

La ricerca di protezione dalle insidie dei nuovi strumenti a disposizione parte, evidentemente, dalla conoscenza della relazione tra i meccanismi di funzionamento delle risorse tecnologiche e la dimensione più strettamente esistenziale degli individui che ne fanno uso.

Al riguardo, dato per presupposto che spazio e tempo rappresentino le dimensioni fondamentali dell'essere, l'evoluzione digitale ha profondamente stravolto i confini esistenziali entro cui l'individuo è storicamente collocato, che assumono ormai una natura evanescente. La dimensione dell'essere oggi prevalente è la rete, che consiste, paradossalmente, in una spazialità a-territoriale. Trattasi, in sostanza, della ridefinizione del "contenitore relazionale" tra individui

che prescinde dall'effettiva prossimità o, più in generale, dal reale calcolo delle distanze, tendenzialmente illimitate nel contesto virtuale.

A sua volta, la percezione del tempo diventa eminentemente attuale, un permanente "qui ed ora" all'interno del quale si realizza una dispersione temporale che è il frutto dell'agitarsi disordinato dell'esperienza nel tempo istantaneo. L'assenza di uno spazio e di un tempo definiti rende le relazioni irrimediabilmente fluide ed esalta all'estremo l'esercizio delle libertà.

Com'è noto, Internet è nato come un sistema interconnesso, fondato su tecnologie comuni; tuttavia, con il tempo, la natura della rete quale *open Internet* si è inquinata. L'espressione "*Internet fragmentation*" è stata utilizzata per la prima volta nel 2015, in occasione del *World Economic Forum*, e si riferisce ad un fenomeno di frantumazione e dispersione che si riflette su diversi aspetti tecnici, politici o commerciali che si manifestano all'interno della rete. La frammentazione, in senso proprio, non consiste nell'inaccessibilità di determinati contenuti on line, quanto più nella mancanza di interoperabilità da cui discende una carenza di comunicazione e una parcellizzazione delle conoscenze.

Il processo di estrema frammentazione del soggetto e dell'oggetto, collegato alla progressiva irrilevanza dei soggetti intermedi (quali i partiti politici, la Chiesa, la stessa famiglia) ha, quindi, raggiunto il culmine con l'avvento del digitale, che ha destrutturato, altresì, gli ambiti che discendono direttamente dalla dimensione esistenziale, ossia quelli della libertà/possibilità e della doverosità.

Al riguardo, se la libertà può essere definita, in un'accezione basica, come lo spazio delle possibilità, è evidente che nel contesto digitale le nostre libertà ci appaiano tendenzialmente infinite. Ciò ha un effetto determinante sul fenomeno giuridico che, da sempre, delimita l'ambito del possibile correggendo la definizione di libertà appena citata come lo spazio delle possibilità delimitato da regole con il fine di garantire la pacifica convivenza tra gli individui. In altri termini, nei sistemi democratici il diritto tenta di delimitare i margini delle libertà degli individui attraverso un equilibrio tra diverse istanze, predeterminando e riducendo ad unità la complessità dei potenziali conflitti.

Il progresso tecnologico ha reso questo compito sempre più arduo, per le ragioni sin qui accennate. Diventa, infatti, improbo per il legislatore predeterminare fattispecie astratte rispetto ad attività umane nuove e multiformi, così come imporre un preciso "dover essere" in una realtà talmente conflittuale e frammentata come quella digitale.

In passato, il diritto individuava limiti agevolmente distinguibili all'interno di ambiti di possibilità ben più ridotti rispetto ad oggi. Basti pensare ai discorsi d'odio on line: nel recente passato, limiti spaziali circoscritti riducevano sensibilmente il rischio di offendere centinaia di persone in pochi secondi e rimanere, in molti casi, impuniti. Oggi, l'utente di un *social network* può, invece, riversare

quotidianamente il proprio odio verso categorie intere di individui senza subirne alcuna conseguenza giuridica.

Alla luce di queste considerazioni, emergono, anzitutto, due interrogativi rispetto al rapporto tra fenomeno giuridico e realtà digitale.

L'esercizio delle libertà nella dimensione "virtuale" dev'essere tutelato in misura maggiore rispetto a quelle della realtà off line? In via connessa, il diritto deve profondamente rinnovarsi per trovare nuovi strumenti e modelli regolatori, tenendo conto del mutato contesto tecnologico?

Per rispondere correttamente a queste domande occorre partire da quanto già accennato sulla sopraggiunta inadeguatezza del fenomeno giuridico a predeterminare le fattispecie umane e risolvere i conflitti nel luogo naturale del conflitto permanente, ossia la rete Internet.

Nelle democrazie liberali l'unica reazione possibile è quella di innovare categorie e strumenti di soluzione della complessità senza, tuttavia, stravolgere i fattori di equilibrio che hanno storicamente caratterizzato la tutela dei diritti fondamentali.

In altri termini, devono rimanere invariati l'approccio cognitivista e i parametri costituzionali che hanno consentito di risolvere razionalmente il bilanciamento tra diritti, senza pericolosi scivolamenti verso derive autarchiche di analisi e risoluzione dei conflitti.

Al tempo stesso, vanno profondamente riadattati al contesto tecnologico tempi e modi dell'attività regolatoria, nonché gli ambiti oggettivi di riferimento, attraverso una ridefinizione dell'attuale estensione delle libertà sulla rete.

Prendendo a modello la libertà d'espressione – che rappresenta probabilmente il paradigma fondamentale di questa nuova era dei diritti – occorre preservare la valutazione razionale della sua natura relativa rispetto ad altri interessi dell'ordinamento e mantenere l'individuazione della tutela della dignità umana quale imprescindibile fattore di equilibrio. Risulta, al contempo, indispensabile ridefinire la reale portata di questa libertà nel contesto tecnologico e individuare nuovi meccanismi di tutela che non subiscano, ma padroneggino, i tempi e gli spazi del mondo digitale.

2. Le trasformazioni delle fonti del diritto nella dimensione digitale. Un'introduzione

2.1. La regolazione attraverso soft law *e* fast law

Come accennato, le nuove tecnologie nel settore dell'informazione e delle comunicazioni sono oggi indispensabili per lo svolgimento di molteplici attività umane: dalle semplici funzioni relative all'individuazione delle preferenze del singolo individuo alla gestione complessa di interessi collettivi. In sostanza,

l'evoluzione tecnologica ha dato vita ad una nuova forma di potere: la capacità digitale di produrre unilateralmente effetti rilevanti nella sfera giuridica di un individuo. Per certo, i sistemi tecnologici attuali incidono sulle libertà fondamentali del singolo, potendo, talvolta, estenderne l'area di esercizio o, in altri casi, restringerla.

In questo nuovo contesto, emerge una questione di carattere costituzionale di non facile soluzione: in che misura è limitabile il nuovo potere tecnologico? E con quali fonti normative, in particolare, laddove il suddetto potere coinvolga i diritti e le libertà fondamentali?

La questione assume una natura costituzionale (Feroni 2022) poiché essa si riferisce, anzitutto, alla forma di stato, per tale intendendosi la soluzione che offre un determinato ordinamento costituzionale per risolvere il conflitto tra autorità e libertà individuali. Com'è noto, il nuovo potere tecnologico può comprimere le libertà fondamentali degli individui in modo diverso rispetto al passato. Basti pensare che nell'Ottocento tale limitazione proveniva dal potere privato del Re, mentre nel Novecento da quello pubblico dello Stato. In entrambi i casi, le restrizioni erano esterne alla sfera personale dell'individuo e alla sua volontà.

Il potere tecnologico interferisce, invece, con i diritti fondamentali attraverso forme diverse: in tal senso, emergono le criticità derivanti dall'accesso alle informazioni attraverso le piattaforme social, senza più l'intermediazione di strutture educative finalizzate a creare un proprio senso critico, necessario per tutelare i singoli dalla disinformazione. Inoltre, come anticipato, le tecnologie stanno sostituendo sempre di più l'attività umana nella fase decisoria delle procedure. Appare quindi evidente che il potere tecnologico – sia laddove offra all'uomo le informazioni necessarie per adottare una decisione, sia laddove lo sostituisca per formularla direttamente – comprime la libertà non dall'esterno, ma dall'interno della volontà. Inoltre, appare necessario considerare la colossale dimensione economica di coloro che sviluppano, producono e mettono in commercio i servizi tecnologici. Ciò rileva indubbiamente ai fini del rapporto tra autorità e libertà – come detto, alla base della definizione di forma di stato – poiché coloro che interferiscono con le nostre libertà sono soggetti privati, creatori e detentori delle più evolute risorse tecnologiche.

Per individuare le possibili forme di limitazione normativa del fenomeno tecnologico vanno tenute in considerazione anche le trasformazioni della forma di governo, per tale intendendosi la distribuzione dei poteri pubblici all'interno di un determinato assetto costituzionale. Il potere tecnologico mette in crisi anche questo aspetto: gli strumenti normativi, tradizionalmente in mano agli organi di rappresentanza politica, sembrano oggi inadeguati a gestire la dimensione digitale e a creare un ordine giuridico conforme ai principi costituzionali (Simoncini 2021).

Ed invero, negli ultimi decenni sono emerse nuove forme di regolazione, quali gli strumenti di *soft-law* (codici etici, dichiarazioni di principi, libri bianchi, etc.)

o, in misura ancora più incisiva, fonti c.d. di *fast law*, riconducibili essenzialmente ad atti regolamentari, di natura non solo tecnica, provenienti da autorità indipendenti o agenzie pubbliche.

Le ragioni di queste nuove forme di regolazione risiedono nell'accennata esigenza di tenere il passo, sempre più veloce e imprevedibile, degli eventi nella dimensione digitale, ricorrendo a competenze e modalità di azione che gli organi rappresentativi non possiedono pienamente. Da qui, il dibattito sull'introduzione di diverse forme di regolazione, in cui non vi è più solo spazio per una eteronormazione di carattere pubblico, ma anche per modelli di autoregolamentazione e co-regolamentazione che coinvolgono soggetti privati.

Queste nuove scelte regolatorie diventano, quindi, necessarie per snellire, modellare e rendere più efficiente la disciplina di settori caratterizzati da forte dinamismo. Esse innovano il sistema e consentono di adeguare la normativa ai cambiamenti sociali e anche alle eventuali sollecitazioni che provengono dall'Unione Europea.

Con riferimento all'ordinamento italiano, lo sviluppo delle anzidette fonti atipiche è, da sempre, legato all'affermarsi del ruolo delle Autorità amministrative indipendenti, quale peculiare modello di azione ed organizzazione amministrativa, chiamate a svolgere compiti di regolazione in ambiti caratterizzati da un elevato grado di competenza tecnica (Bucalo 2018). Più di recente, il dibattito ha assunto una dimensione più ampia, per il rafforzamento dei poteri normativi (Tedesco 2023), anche in ambiti non strettamente tecnici, di alcune Autorità indipendenti, quale l'ANAC, nonché per il riconoscimento di altrettanto forti poteri regolatori ad agenzie governative, quale l'Agenzia per l'Italia digitale, proprio nell'ambito dell'innovazione e della digitalizzazione.

Parallelamente, è indubbio il ruolo di crescente protagonismo che le Autorità amministrative indipendenti stanno assumendo nella regolazione delle applicazioni pratiche dei sistemi tecnologici (Simoncini 2021). Basti pensare, ad esempio, al Garante per la protezione dei dati personali, all'Autorità per le garanzie nelle comunicazioni, all'Autorità garante della concorrenza e del mercato, che sono sempre più frequentemente chiamate, dalla normativa europea e dalla legislazione interna, a verificare il rispetto delle norme riguardanti i nuovi fenomeni tecnologici e digitali. La regolazione attraverso le *Authority* e le agenzie rappresenta quindi un paesaggio complesso, nel quale si moltiplicano i centri di produzione del diritto e i soggetti chiamati a darvi attuazione o a garantirne l'osservanza.

È qui che appare chiara la trasformazione del sistema delle fonti imposta dall'avvento del paradigma tecnologico e dal suo impatto su forme di stato e forme di governo. Grazie a questi nuovi modelli regolatori si tenta di definire il limite entro cui la tecnologia può interferire sulle libertà fondamentali e, al contempo, si fissa un nuovo assetto nella distribuzione del potere di regolazione pubblica.

2.2. La Dichiarazione dei diritti su Internet come primo tentativo di ridefinire l'ambito oggettivo dei diritti fondamentali

Nel 2014, l'allora Presidente della Camera Laura Boldrini nominò una Commissione di studio presieduta da Stefano Rodotà per adottare una Dichiarazione dei diritti su Internet che fosse largamente condivisa e potesse trovare attuazione in un ambito più ampio di quello nazionale. In particolare, lo scopo era quello di introdurre nuove forme di regolamentazione, diverse dal tradizionale modello normativo composto da regole e sanzioni, attraverso un approccio incentrato su principi generali con cui bilanciare gli interessi in gioco. La Commissione formulò un testo della Dichiarazione sottoposto a consultazione pubblica e poi pubblicato sul sito ufficiale della Camera.

Era la prima volta che il Parlamento promuoveva una Commissione di studio di questo tipo poiché nessuna legge o disposizione del regolamento della Camera dei deputati attribuiscono al Presidente il potere di nominare un gruppo di lavoro di tal genere. L'intenzione era evidentemente quella di portare all'attenzione dei decisori politici il tema dei diritti e dei doveri sulla rete, considerato, peraltro, che la Dichiarazione non aveva valore normativo, ma era stata disegnata come strumento di *soft law* per orientare e indirizzare l'organo politico nell'adozione di determinate decisioni.

L'art. 1 della Dichiarazione ribadisce l'intenzione di garantire i diritti fondamentali già riconosciuti da una pluralità di fonti, ivi incluse quelle sovranazionali. Trattasi di un rinvio generico, che equipara molteplici documenti dal valore giuridico diverso. L'articolo prevede due criteri per interpretare i suddetti diritti: il bilanciamento tra diritti differenti si deve fondare sul rispetto della dignità, libertà e uguaglianza, e gli stessi diritti devono essere interpretati al fine di favorirne l'effettività.

L'art. 2 tutela il diritto di accesso a Internet, sancendo come ogni persona sia titolare di tale diritto in condizioni di parità, con modalità tecnologiche adeguate e aggiornate; trattasi, quindi, di uno strumento giuridico idoneo a superare il divario digitale, inteso come ostacolo al pieno sviluppo della persona e strettamente connesso al principio di eguaglianza sostanziale di cui all'art. 3, comma 2, Cost.

Il problema degli ostacoli che si interpongono all'accesso a Internet è richiamato dall'art. 3, che prevede il diritto alla conoscenza e all'educazione in rete, affinché sia promosso un uso consapevole di Internet. In tal senso, il testo recita che «ogni persona ha diritto ad essere posta in condizione di acquisire ed aggiornare le capacità necessarie ad utilizzare Internet in modo consapevole per l'esercizio dei propri diritti e delle proprie libertà fondamentali».

L'art. 4 introduce il principio della neutralità della rete (cd. *net neutrality*), secondo il quale ogni persona ha diritto a che i propri dati, trasmessi o ricevuti su Internet, non subiscano discriminazioni o interferenze in base a mittente, ricevente, contenuto, dispositivo utilizzato o legittime scelte delle persone.

L'art. 5 (tutela dei dati personali), l'art. 6 (diritto all'autodeterminazione informativa) e l'art. 8 (trattamento automatizzato dei dati personali) si incentrano su principi già riconosciuti dalle disposizioni nazionali e sovranazionali; l'art. 7 sembra introdurre una riserva di giurisdizione, sancendo l'inviolabilità dei sistemi e dei dispositivi informatici di ogni persona, così come la libertà e la segretezza delle sue informazioni e comunicazioni elettroniche, salvo deroghe nei soli casi e modi stabiliti dalla legge e con l'autorizzazione motivata dell'autorità giudiziaria. Appare evidente l'intento di estendere al web le garanzie previste dagli artt. 14 e 15 Cost.

L'art. 9 prevede il diritto all'identità digitale; l'art. 10 sancisce la protezione dell'anonimato, salvo limitazioni necessarie, proporzionate, fondate sulla legge e giustificate dall'esigenza di tutelare gli interessi pubblici rilevanti; l'art. 11 concerne il diritto all'oblio; l'art. 12 impone il dovere di lealtà e correttezza dei responsabili delle piattaforme digitali nei confronti di consumatori ed utenti; l'art. 13 garantisce la sicurezza in rete e l'integrità delle infrastrutture e la loro tutela da attacchi, richiamando la legittimità di limitare la libertà di manifestazione del pensiero laddove essa si traduca in discorsi d'odio.

Concludendo, l'art. 14 include un ampio numero di obiettivi che devono essere perseguiti nella realizzazione delle politiche di *governance*. Nello specifico, l'articolo rinvia all'esigenza di costruire regole universali e internazionali concernenti Internet ai fini dell'attuazione dei diritti e principi indicati, garantendone il carattere aperto e democratico.

Per certo, la Dichiarazione in esame ha rappresentato una scelta innovativa da un punto di vista culturale, tentando di codificare i nuovi diritti emergenti nell'era di Internet ed avviare un percorso di ridefinizione dell'ambito oggettivo di quelli tradizionali. Ferma restando l'opinabilità della tecnica redazionale prescelta, a metà strada tra un mero elenco e una disciplina tecnica, e la totale assenza di valore precettivo, la Dichiarazione rappresenta comunque un primo testo significativo verso il passaggio a nuovi modelli di individuazione e tutela dei diritti fondamentali nel contesto tecnologico (Nannipieri 2014).

3. Piattaforme digitali e diritti fondamentali. Un'introduzione

Internet è una comunità mondiale che si articola in numerose piattaforme interconnesse e tra loro differenti, le quali includono 4 miliardi di persone; nello specifico, secondo il rapporto annuale di *We Are Social*, più del 64% della popolazione mondiale ha avuto accesso al web nel 2023, ossia circa 5,16 miliardi di persone.

La globalizzazione digitale deve chiaramente fare i conti con i diversi contesti territoriali in cui operano gli utenti, caratterizzati da sensibilità e criticità

differenti. La Convenzione di Budapest sul *cybercrime* è un esempio di un quadro regolatorio più esteso che uniforma definizioni esistenti in contesti differenti. Ciò sta avvenendo, ad esempio, anche in tema di dati personali o di intelligenza artificiale, in cui concetti tecnici si affiancano a nozioni più elastiche di natura giuridica che, per definizione, devono comunque essere generali e astratte, seppur generalità e astrattezza siano caratteristiche che spesso confliggono con la precisione tipica delle regole tecniche (Corasaniti 2021).

Sennonché, la diffusione e l'influenza dalle piattaforme digitali appaiono inarrestabili. Le *platforms* si sono dimostrate un centro di interazione sociale e di comunicazione globale, con un'elevata capacità di influire anche sulla regolazione e sul controllo delle condotte degli utenti, tanto da adottare proprie *policies* di autoregolazione e procedure di verifica e sanzione delle violazioni commesse. I differenti sistemi giuridici devono, quindi, costantemente confrontarsi con le piattaforme che diventano una sorta di tribunale speciale all'interno di un territorio fertile di odio, ostilità e intolleranza (Pollicino 2020).

Emerge così una questione complessa, dai contorni sovranazionali, in quanto il potere riconosciuto ai *social network* rischia di rimanere al di fuori del controllo delle più autorevoli istituzioni internazionali.

Le strade sin qui percorse, a livello nazionale e, soprattutto, europeo, per contenere il rischio di asimmetrie regolatorie o, financo, di vuoti normativi sono state diverse e, in taluni casi, decisamente innovative.

Il tentativo più rilevante di mediare tra autonomia delle piattaforme e dominio pubblico della produzione normativa è stato promosso dalla Commissione europea attraverso l'adozione, nel 2016, di un Codice di condotta per combattere l'incitamento all'odio on line e, nel 2018, di un Codice di condotta sulla disinformazione, quali esempi di co-regolamentazione e di etero-controllo sulle condotte degli utenti (Calimà 2020). In particolare, la Commissione ha inteso coinvolgere gli *stakeholders* nella fase di elaborazione dei principi necessari per realizzare una disciplina comune della materia e affidare alle stesse piattaforme un ruolo da protagonista nel garantire il rispetto di tali regole.

A livello interno, l'Autorità per le garanzie delle comunicazioni ha promosso l'istituzione di un Tavolo tecnico per la garanzia del pluralismo e della correttezza dell'informazione sulle piattaforme digitali (AGCOM 2017), al fine di identificare gli obiettivi e gli strumenti migliori da utilizzare per garantire la correttezza dello svolgimento della campagna elettorale. L'AGCOM, durante la campagna per le elezioni politiche del 2018, ha ritenuto opportuno adottare linee guida che assicurassero la parità di accesso alle piattaforme on line (tra queste, *Google* e *Facebook*). Tali piattaforme, attraverso procedure di autoregolamentazione, hanno introdotto misure idonee a reprimere la diffusione e condivisione on line di contenuti che violassero i principi connessi al pluralismo dell'informazione.

Nonostante siano emersi alcuni risultati apprezzabili da queste forme di collaborazione tra autorità pubbliche e piattaforme private, e in particolare un maggior impegno dei principali *social network* per la rimozione di contenuti palesemente discriminatori o ingannevoli, la scarsa capacità coercitiva di queste fonti di *soft law* è, alla lunga, emersa. Per certo, tali strumenti sono apprezzabili in quanto più adattabili e flessibili; ciononostante, l'estrema rapidità dei mutamenti comportamentali degli utenti di fronte a sempre nuovi strumenti digitali (si pensi all'IA generativa) hanno imposto modelli più strutturati ed efficaci di rimozione e segnalazione dei contenuti, in grado di restituire al potere pubblico la sovranità sulla produzione normativa e sul controllo giurisdizionale delle condotte umane.

Lo stesso Mark Zuckerberg, CEO di *Facebook*, ha ammesso come sia indispensabile un ruolo attivo dei governi e dei regolatori pubblici, in quanto solo la regolamentazione "esterna" e tradizionale può aiutare i *social* a stabilire il proprio ambito di competenza rispetto a fenomeni complessi quali il contrasto alle discriminazioni, la tutela della *privacy* e la disinformazione on line (Bonini 2020).

I recenti pacchetti normativi approvati dall'Unione Europea in materia di dati e servizi digitali, e in particolare il *Digital Services Act* (di cui si parlerà nella Lezione II), hanno fissato nuove e più articolate regole per affidare a piattaforme ed utenti procedure di controllo più snelle e, al tempo stesso, efficaci, attraverso un bilanciamento – ben visibile anche in relazione al recentissimo AI Act – tra rafforzamento del mercato digitale e tutela dei diritti fondamentali.

4. Nuovi fenomeni on line

4.1. Il cyberbullismo

Come accennato, uno degli effetti più radicali della rete è quello di annullare le distanze, almeno apparentemente. Ciò ha cambiato le modalità di interazione sociale concedendo, da un lato, spazi di libertà considerevolmente più ampi ma dando spazio, dall'altro, a nuove e pericolose condotte illecite.

Tra queste, va, anzitutto, citato il cyberbullismo, quale fenomeno strettamente connesso alle nuove relazioni digitali, che escludono la partecipazione del corpo nella sua fisicità, favorendo pensieri e comportamenti più espansivi e incrementando l'aggressività, specie nei più giovani.

L'interconnessione tra dispositivi ha così mutato il bullismo inteso in senso tradizionale, che ha assunto nuove forme on line. Il termine è stato coniato dall'educatore Bill Belsey nel 2004, che lo ha riferito a quei comportamenti ostili e intenzionali tenuti da singole persone o da gruppi per danneggiare altri individui attraverso le tecnologie informatiche di comunicazione.

La realtà digitale è diventata così coinvolgente che può essere definita come una ragnatela (Ammaniti - Ammaniti 2015), che intrappola i ragazzi all'interno di questa nuova dimensione; ed è proprio per tale ragione che il cyberbullismo ha un maggiore impatto emotivo rispetto al bullismo tradizionale. In particolare, gli effetti del fenomeno in esame non si limitano al presente, ma si estendono anche al futuro, a causa della permanenza dei contenuti condivisi on line, che possono rimanere attivi sul web per lunghi periodi, assumendo anche formati diversi e diffondendosi tra varie piattaforme. Al riguardo, il cyberbullismo – diversamente dal bullismo tradizionale – non richiede che l'azione sia ripetuta; una singola aggressione on line è sufficiente per ripetersi, diffondersi ed essere condivisa fra le molteplici piattaforme.

Un'ulteriore caratteristica, assai frequente, del cyberbullismo è l'anonimato dell'aggressore; anonimato che riduce o annulla l'inibizione sociale dell'aggressività. Il cyberbullo non ha autocontrollo in quanto la sua identità è ignota: egli non percepisce la pressione di osservare i canoni sociali di rispetto dell'altra persona e non ha timore di essere perseguito dalle autorità (Genta 2017). La superiorità fisica sulla vittima – tipica del bullismo tradizionale – assume in rete un ruolo secondario, data la dematerializzazione del rapporto on line. Tale dematerializzazione del rapporto on line determina una depersonalizzazione della vittima, che viene deumanizzata dal cyberbullo; ciò, provoca una minimizzazione dell'importanza aggressiva dell'atto tale da provocare un senso di irresponsabilità per l'aggressore (Francese 2022).

Esistono numerose tipologie di cyberbullismo. Vanno citati, a titolo esemplificativo, il *flaming* (messaggi on line violenti per umiliare i destinatari), il *cyberstalking* (analogamente allo *stalking*, consiste in molestie ripetute e serie minacce per spaventare la vittima), la *denigration* (messaggi e commenti on line finalizzati ad emarginare ed isolare la persona).

Il cyberbullismo è, quindi, ritenuto meritevole di autonoma considerazione, in ragione di specifiche caratteristiche che hanno indotto il legislatore a trattarlo come fattispecie a sé, attraverso un'apposita disciplina. Nella legge n. 71/2017, concernente le disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo, quest'ultimo viene definito come «qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo». La legge individua, pertanto, una serie di misure di carattere preventivo ed educativo nei confronti

dei minori (qualunque sia il ruolo nell'episodio) da attuare in ambito scolastico, e non solo.

Va, inoltre, dato rilievo a una disciplina speciale della collaborazione tra autorità pubbliche e piattaforme digitali, laddove è previsto che il minore (ma maggiore di 14 anni, in caso contrario sarà rappresentato dai genitori) possa chiedere al gestore della piattaforma di rimuovere, bloccare o oscurare i contenuti di cyberbullismo. Se la *platform* non provvede entro 48 ore, la vittima potrà rivolgersi al Garante per la protezione dei dati personali che interviene entro le successive 48 ore.

4.2. Il revenge porn

Tra le condotte illecite nate a seguito dell'evoluzione digitale emerge sempre più prepotentemente il *revenge porn*. L'espressione, che associa la parola "vendetta" a quella di "porno/pornografia", lascia facilmente intendere il suo significato: trattasi della divulgazione on line non consensuale di contenuti multimediali pornografici o, comunque, di natura intima o sessuale, che ledono la riservatezza della persona.

Sono in aumento anche i casi di *sextortion*, che consistono nel ricattare la vittima di pubblicare foto o video sessualmente espliciti qualora essa non soddisfi le richieste dell'aggressore.

A causa delle dimensioni preoccupanti che ha assunto il fenomeno, il legislatore è già intervenuto in molti Paesi, tra cui, Inghilterra, Israele, Canada, Australia, Giappone, diversi Stati degli USA e anche l'Italia.

La legge n. 69/2019 (il cd. Codice Rosso) ha introdotto nel Codice Penale l'art. 612-*ter* rubricato "Diffusione illecita di immagini o video sessualmente espliciti". La disposizione è stata inserita nella Sezione III del Codice penale, dedicata ai delitti contro la libertà morale, e a sua volta prevista nel Capo III (Dei delitti contro la libertà individuale) del Titolo XII del Codice Penale (Delitti contro la persona).

L'art. 612-*ter* c.p. è definito "a doppio binario" poiché prevede due commi distinti che perseguono il medesimo scopo: punire la diffusione di contenuti sessualmente espliciti senza consenso.

Il primo comma sanziona chiunque, «dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video sessualmente espliciti, destinati a rimanere privati, senza il consenso delle persone rappresentate». In sostanza, l'agente è colui che diffonde video che lui stesso ha realizzato o che ha sottratto all'altra persona senza il suo consenso.

Il secondo comma ha una portata diversa, punendo colui che «avendo ricevuto o comunque acquisito le immagini o i video li invia, consegna, cede, pubblica o diffonde senza il consenso delle persone rappresentate al fine di recare

loro nocumento». Qui, il soggetto agente non realizza o sottrae i contenuti, ma li riceve e li diffonde senza il consenso della vittima per perseguire uno scopo preciso: recarle nocumento.

Il terzo e quarto comma prevedono due circostanze aggravanti: la prima sussiste quando la diffusione del materiale sia realizzata dal coniuge, anche se separato o divorziato, o da persona legata alla vittima da una relazione affettiva, ovvero qualora siano utilizzati strumenti informatici o telematici per la condivisione. La seconda, si riferisce ai casi in cui la vittima sia una persona in condizione di inferiorità fisica o psichica o una donna in stato di gravidanza.

Com'è noto, il *revenge porn* lede la riservatezza, la reputazione e l'onore della persona. In ragione di ciò, l'art. 144-*bis* del Codice in materia di protezione dei dati personali riconosce una specifica competenza al Garante per la protezione dei dati personali cui può rivolgersi, mediante segnalazione o reclamo, «chiunque, compresi i minori ultraquattordicenni, abbia fondato motivo di ritenere che immagini o video a contenuto sessualmente esplicito che lo riguardano, destinati a rimanere privati, possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione senza il suo consenso in violazione dell'articolo 612-*ter* del Codice penale». L'Autorità, entro 48 ore dalla ricezione della richiesta, predispone le indagini, trasmettendo al Pubblico Ministero la suddetta segnalazione e la documentazione acquisita, come previsto dall'art. 58 GDPR. Tuttavia, la segnalazione di cui al comma 1 nei confronti del Garante per la protezione dei dati personali non corrisponde automaticamente ad un'incriminazione del reato *ex* art. 612-*ter* c.p.

I gestori delle piattaforme digitali devono conservare il materiale oggetto di contestazione a fini probatori, in conformità con le misure stabilite dal Garante finalizzate ad impedire che gli interessati siano riconosciuti. In caso di inadempimento, l'Autorità dovrà diffidare il fornitore delle piattaforme; laddove ci fosse inottemperanza alla diffida si applicherà una sanzione amministrativa pecuniaria (Martorana - Sichi 2022).

4.3. Il deepfake

I *deepfake* sono un fenomeno recente e fortemente variegato. Il termine consiste nell'accostamento della parola "*fake*" alla nozione di "*deep learning*": trattasi di contenuti falsi (video, immagini o audio) prodotti dall'intelligenza artificiale e, in particolare, da meccanismi di *deep learning* per rendere il risultato altamente realistico. Questa pratica di manipolazione non colpisce solo la vittima diretta ma anche lo spettatore, il quale assume un ruolo primario nel promuovere la circolazione del materiale.

La potenzialità del danno dei *deepfake* si incentra sulla loro verosimiglianza: sono contenuti diretti a far sembrare vero ciò che non è mai accaduto. L'efficacia consiste nella loro apparente trasparenza, che consente di screditare un soggetto

imputandogli comportamenti o dichiarazioni false per ottenere la più ampia condivisione dallo spettatore, che lo diffonderà sulla rete. Gli scopi perseguiti possono essere molteplici: intimidazione, bullismo, finalità politiche e così via.

Appare quindi evidente la potenzialità lesiva di tale fenomeno; la manipolazione dei contenuti non si limita a violare la sfera privata dell'individuo, ma rappresenta un serio pericolo per un'intera comunità dato che i *deepfake* risultano tra gli strumenti più efficaci per diffondere *fake news* e disinformazione.

Il fenomeno del *deepfake* incrocia, a volte, quello del *revenge porn*. Trattasi dei *deepnude*, per tali intendendosi i contenuti falsi con cui volti o corpi di persone (anche minorenni) sono manipolati e sovrapposti sui corpi di altri soggetti nudi o in pose o atti di natura esplicitamente sessuale (Viola - Voto 2022).

Ad oggi, l'unico rimedio normativo opportuno per affrontare un simile fenomeno è il nuovo regolamento europeo sull'intelligenza artificiale. L'*Artificial Intelligence Act* non vieta in modo assoluto i *deepfake*, ma impone alcuni requisiti minimi di trasparenza nei confronti di chi li realizza. Tuttavia, l'*AI Act* prevede alcune eccezioni, laddove l'uso sia «autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati o, se è necessario, per l'esercizio del diritto alla libertà di espressione e del diritto alla libertà delle arti e delle scienze garantito dalla Carta dei diritti fondamentali dell'UE, e fatte salve le tutele adeguate per i diritti e le libertà dei terzi».

Pertanto, ad oggi non esiste un quadro normativo esaustivo in grado di affrontare e contrastare i *deepfake* nonostante viviamo in un periodo storico in cui non è più così certo che cosa sia falso e che cosa non lo sia. Ciò mette a rischio la tenuta stessa delle nostre democrazie: la percezione della realtà è costantemente alterata, ciascun individuo tende sempre più a credere solo a ciò che considera soggettivamente vero, con effetti che si riverberano inevitabilmente sulla formazione dell'opinione pubblica e sulla reale conoscenza e consapevolezza dei contesti sociali e politici (Azzalli - Ellecosta 2024).

5. Prospettive distopiche e neo-costituzionalismo digitale

Le potenzialità di una realtà digitale parallela sono ben note. Basti pensare all'industria dei videogiochi, all'utilizzo del mondo virtuale per la progettazione e costruzione di nuovi edifici, al mondo del cinema che impiega sosia grafici, alle criptovalute che, prive di materialità, promuovono il progresso monetario dell'universo digitale. Questi rappresentano solo frammenti di ciò che diventerà un meta-universo onnicomprensivo.

All'inizio dell'era digitale, il funzionamento tecnologico si fondava sui *computer*, oggi sugli *smartphone*, domani sull'individuo stesso, attraverso visori, realtà aumentata, *microchip* sottocutanei.