ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

Scuola di Scienze
Corso di Laurea in Ingegneria e Scienze Informatiche

L'ANONIMATO NELL'ERA DIGITALE: DIFFERENZE, RAGIONI E APPROCCI PER SALVAGUARDARE L'IDENTITÀ DIGITALE

Elaborato in
Informatica E Diritto

Relatore
Prof. ssa Luisa Dall'Acqua

Presentata da
Enea Bresciani

Terza Sessione di Laurea
Anno Accademico 2023 – 2024

PAROLE CHIAVE

Anonimato digitale

Identità online e privacy

Regolamentazione dei social media

Verifica dell'identità sui social

Comportamenti antisociali e anonimato

I social media danno diritto di parola a legioni di imbecilli che prima parlavano solo al bar dopo un bicchiere di vino, senza danneggiare la collettività. Venivano subito messi a tacere...
Umberto Eco

Ringraziamenti

Per prima cosa, vorrei ringraziare la mia relatrice, la Prof. ssa Luisa Dall'Acqua, per i suoi preziosi consigli e per la sua disponibilità. Grazie per avermi fornito spunti fondamentali nella stesura di questo lavoro e per avermi indirizzato nei momenti di indecisione. Ringrazio infinitamente i miei familiari, che mi hanno sempre motivato a dare il meglio.

Indice

Introduzione

Nell'odierna società digitale, i social media sono diventati non solo una piattaforma di comunicazione, ma anche un luogo virtuale in cui si riflettono e si amplificano le dinamiche sociali del mondo reale. L'interconnessione permessa da piattaforme come Meta (Facebook e Instagram), X (ex Twitter) e TikTok ha modificato radicalmente il modo in cui le persone interagiscono, si informano e costruiscono la propria identità. Tuttavia, questo cambiamento ha sollevato questioni importanti legate alla *privacy* e alla gestione dell'identità, introducendo concetti complessi come l'anonimato e l'autenticità online. Molti utenti scelgono di nascondere parzialmente o completamente la propria identità digitale, per proteggere la propria *privacy* o per sentirsi liberi di esprimere opinioni altrimenti non accettate socialmente o politicamente.

Da un lato, l'anonimato offre numerosi vantaggi, tra cui la protezione dalla sorveglianza e dal giudizio pubblico, la tutela della libertà di espressione e uno spazio sicuro in cui riflettere e sperimentare. Tuttavia, esso porta con sé anche una serie di rischi e criticità. Senza un'identità chiara, gli utenti possono essere spinti a comportamenti antisociali e dannosi, come l'incitamento all'odio, il bullismo e la disinformazione, che si diffondono facilmente nei contesti *online*. Questo fenomeno rappresenta una sfida non solo per le piattaforme stesse, ma anche per le istituzioni che regolano lo spazio digitale e i diritti degli utenti.

Questa tesi ha l'obiettivo di analizzare le ragioni che portano gli utenti a cercare l'anonimato online, focalizzandosi sulle implicazioni legali, sociali e psicologiche di tale scelta. Particolare attenzione sarà dedicata all'analisi normativa, che esplorerà i principali strumenti di protezione dei dati e le normative sull'anonimato online, con riferimento alle direttive internazionali e alle regolamentazioni nazionali ed europee. Attraverso un confronto approfondito tra i contratti di utilizzo delle principali piattaforme social, come Meta, X e TikTok, verranno messe in luce le diverse modalità con cui questi colossi digitali gestiscono la *privacy* e l'identità degli utenti. In un mondo in cui le piattaforme social rappresentano ormai un prolungamento delle interazioni pubbliche, comprendere le dinamiche e le limitazioni dell'anonimato risulta fondamentale per una valutazione equilibrata tra libertà individuale e responsabilità sociale.

Infine, nella parte conclusiva della tesi, verrà esaminata la possibilità di

adottare un sistema di verifica dell'identità online che permetta agli utenti di preservare la loro *privacy*, mantenendo comunque la responsabilità delle loro azioni. In questa prospettiva, i social media vengono paragonati ai tradizionali luoghi di ritrovo, come i bar o le piazze, dove le persone interagiscono esponendosi con la propria identità, contribuendo a una convivenza più rispettosa e civile. Tale paragone permette di introdurre una riflessione su come il mondo digitale possa evolversi verso un ambiente simile, dove l'autenticità e la trasparenza diventano i fondamenti di una comunità virtuale responsabile e sicura.

Capitolo 1

Motivazioni e modalità per ricercare l'anonimato online

In questa parte analizziamo le ragioni per cui le persone cercano attivamente di essere anonime online e quali misure solitamente queste mettono in atto.

1.1 Le ragioni per cui le persone cercano l'anonimato online

La protezione della *privacy* è una delle ragioni principali per cui gli utenti cercano l'anonimato *online*. Con la crescente raccolta e utilizzo dei dati personali da parte di aziende e governi, gli utenti vogliono evitare che le loro informazioni sensibili vengano condivise o utilizzate senza consenso. In Italia 8 utenti su 10 si dimostrano preoccupati per la tutela della propria *privacy* e due terzi non hanno fiducia nel rilasciare i propri dati sul web. [1] La paura di essere sorvegliati, sia da enti pubblici che privati, porta molte persone a cercare di nascondere la propria identità per evitare violazioni della propria sfera privata. L'anonimato diventa così uno strumento per mantenere il controllo sui propri dati e proteggersi da intrusioni non autorizzate.

In molti contesti, soprattutto in paesi con regimi autoritari o dove la libertà di parola è limitata, l'anonimato online è essenziale per esprimere opinioni critiche senza timore di ritorsioni per dissidenti politici, giornalisti e *whistleblowers*. Gli utenti sfruttano la possibilità di rimanere anonimi per partecipare a discussioni su temi delicati, denunciare ingiustizie o parlare di argomenti controversi che potrebbero altrimenti esporli a censura o persecuzioni legali. In questi contesti, l'anonimato diventa una forma di protezione essenziale per

garantire la libertà di espressione.

Per molte persone, l'anonimato è una questione di sicurezza personale. Gli utenti che temono per la propria incolumità, come attivisti politici, giornalisti investigativi o vittime di *stalking*, si affidano all'anonimato per proteggersi da minacce reali. Nascondere l'identità è un modo per evitare che le informazioni personali vengano utilizzate per scopi malevoli, inclusi attacchi fisici o digitali.

Il controllo dell'identità digitale è un altro motivo per cui le persone cercano l'anonimato *online*. Gli utenti vogliono poter decidere quali informazioni condividere e con chi. L'anonimato offre loro la libertà di creare e modificare la propria identità in base al contesto, senza sentirsi vincolati alle aspettative della società o delle piattaforme su cui operano.

L'anonimato è parte integrante della cultura di internet, specialmente nelle prime comunità online come i forum, i *newsgroup* e, successivamente, le piattaforme di social media. Su internet, l'anonimato ha favorito la creazione di un ambiente in cui gli utenti si sentivano liberi di esplorare nuove identità, di partecipare a conversazioni che non avrebbero altrimenti potuto avere nella vita reale e di costruire nuove reti sociali. Questo aspetto culturale, radicato nella storia di internet, continua ad essere un motivo per cui molte persone preferiscono mantenere l'anonimato.

1.2 Le tecniche per ottenere l'anonimato: Approcci per utenti medi vs utenti avanzati

1.2.1 Utente medio: Tecniche e strumenti di base per proteggere la privacy

Gli utenti casual che vogliono proteggere la propria *privacy online* utilizzano spesso strumenti semplici e accessibili. Tra questi:

Navigazione in incognito

Molti *browser* moderni prevedono la navigazione in incognito. Questa evita che che si acceda automaticamente agli account salvati e che i dati di navigazione rimangano sul dispositivo dopo aver terminato la navigazione, ma non nasconde in alcun chi stia richiedendo certe pagine o da dove le richieste provengano[2].

Igiene Informatica

Per igiene informatica si intende l'insieme delle buone abitudini da seguire per ridurre al minimo i rischi derivanti dall'utilizzo di un sistema informatico, come ad esempio effettuare tutti gli aggiornamenti *software* appena disponibili o utilizzare password complesse e diverse per ogni servizio[3].

Account Temporanei

Qual'ora fosse obbligatorio registrarsi ad un sito a cui non vogliamo comunicare il nostro indirizzo mail o il nostro numero di telefono è possibile fare ricorso a svariati servizi di email o numeri di telefono temporanei. Solitamente questi servizi sono gratuiti e pur non offrendo la possiblità di inoltrare mail o effettuare chiamate telefoniche, danno la possibilità di ricevere *mail* e sms con codici di conferma.

Crittografia End-to-End

Al fine di mantenere riservate le comunicazioni è possibile ricorrere alla crittografia *End-to-End*. Questo tipo di crittografia rende possibile interpretare i messaggi unicamente al mittente e al destinatario, rendendola incomprensibile a chiunque intercetti i messaggi. Questa tecnica è oggi facilmente utilizzabile da tutti in quanto esistono app di messaggistica dedicate (come ad esempio *Signal*) oppure lo standard *OpenPGP* (derivato dalla *suite di software Pretty Good Privacy*) utile per cifrare e autenticare le mail.

VPN (Virtual Private Network)

Ad oggi, uno dei prodotti più pubblicizzati per tutelare la propria privacy navigando in rete sono le VPN (*Virtual Private Network*). Queste permettono di creare un tunnel crittografato tra il dispositivo dell'utente e il server VPN, nascondendo l'indirizzo IP dell'utente e la sua posizione. Grazie a ciò il nostro ISP non sarà più in grado di monitorare il nostro traffico (ma saprà che stiamo usando una VPN) e di fornire un IP e posizione non veritiere al servizio al quale ci stiamo collegando. Tuttavia a questi servizi, in quanto commerciali, le autorità possono richiedere di rivelare i dati di utilizzo del servizio VPN. Solitamente i servizi VPN non tengono traccia dei dati di navigazione, ma unicamente di chi e quando ha fatto uso del servizio. Da qui le autorità, incrociando date e orari, sono in grado di assegnare ad ogni utente il proprio traffico.

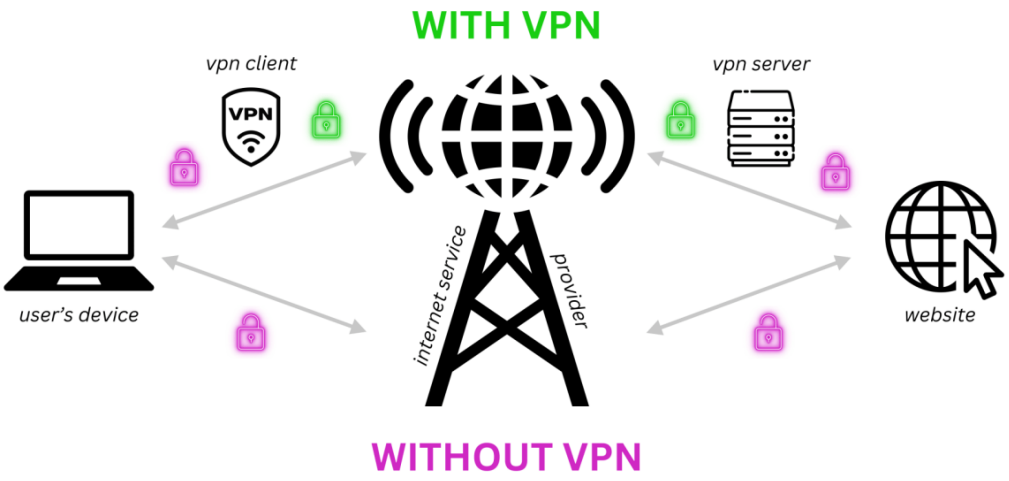

Figura 1.1: Schema che illustra la differenza tra la connessione internet con e senza l'uso di una VPN (Virtual Private Network).[4]

Pseudonimi

Utilizzare nomi falsi o pseudonimi per interagire online è una pratica comune e diffusa. Questo permette di potersi esprimere *online* senza che la nostra identità sia nota a tutti. Questo però non impedisce in alcun modo al ISP o alle autorità di sapere da dove stiamo operando e cosa stiamo facendo.

1.2.2 Utente avanzato: Misure più sofisticate per garantire l'anonimato

Gli utenti avanzati adottano strategie molto più complesse e sofisticate per mantenere l'anonimato, spesso per proteggersi da attori con risorse maggiori, come governi o gruppi criminali. Alcune delle tecniche includono:

Tor (The Onion Router)

Tor è un *software* con lo scopo di permettere una navigazione completamente anonima sul web. Si basa sul protocollo di rete Onion Routing. Questo protocollo si basa sul far criptare e decriptare il messaggio ad ogni router che questo attraversa con una chiave diversa.

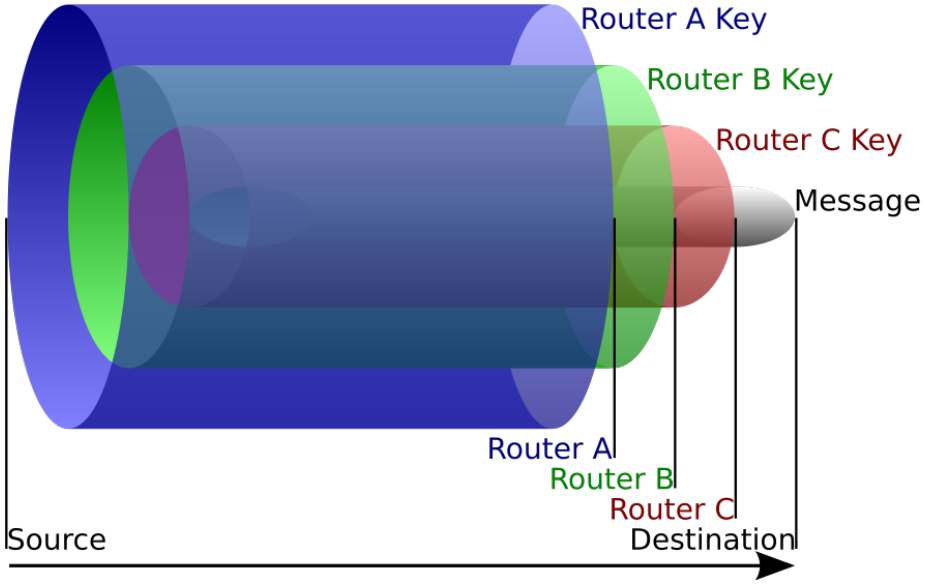

Figura 1.2: In questo esempio il mittente manda i dati al Router A, e inoltra il pacchetto privo dello strato A al Router B e così via. Il Router C infine invia al destinatario il messaggio decriptato. I Router non sanno se il messaggio arriva da un Router mittente o un Router intermediario.[5]

L'autore originale del messaggio rimane segreto in quanto ogni nodo conosce solo il precedente e successivo (tranne il primo nodo che conosce il mittente e l'ultimo nodo che conosce il destinatario). Tor sarebbe un sistema virtualmente perfetto se operasse con un numero altissimo di nodi (nell'ordine delle centinaia di migliaia), decentralizzati e P2P. Tuttavia, poiché i nodi sono gestiti da volontari, in genere funziona con qualche migliaio di nodi, con una dispersione geografica limitata, spesso concentrata nei data center. Tor quindi non ha una struttura completamente decentralizzata e P2P, in quanto è necessaria la presenza di nodi stabili per garantire il funzionamento della rete in ogni momento. Questo rende la rete vulnerabile a degli attacchi *End to End*, dove l'attaccante possiede sia il nodo iniziale che il nodo finale. È noto che l'NSA riesce ad attaccare la rete Tor in questo modo[6].

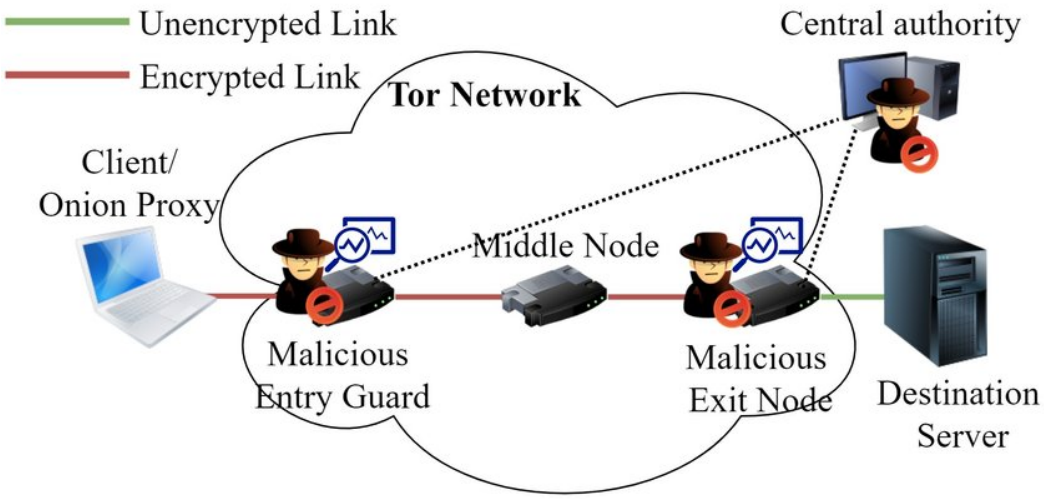

Figura 1.3: Scenario di attacco End to End, dove l'attaccante possiede sia il nodo di ingresso che quello di uscita, riuscendo così a deanonimizzare il traffico.[7]

Tails OS

Esistono anche sistemi operativi incentrati sul proteggere la *privacy* degli utenti. Tails (*The Amnesic Incognito Live System*) OS è un sistema operativo pensato per massimizzare la *privacy* degli utenti. Tails è stato progettato per non essere installato direttamente su una macchina, ma per essere eseguito direttamente da una chiavetta USB, in modo da non lasciare nessuna traccia sul computer in cui viene usato. Inoltre usa di defult la rete Tor, anonimizzando tutto il traffico proveniente dal sistema operativo, non solo la navigazione web.

Modificare gli indirizzi fisici e codici univoci della macchina

Un altro modo per occultare la nostra identità *online* consiste nel modificare gli indirizzi fisici delle schede di rete dei dispositivi. Ogni scheda di rete ha un suo indirizzo MAC univoco, associato al produttore della scheda stessa.

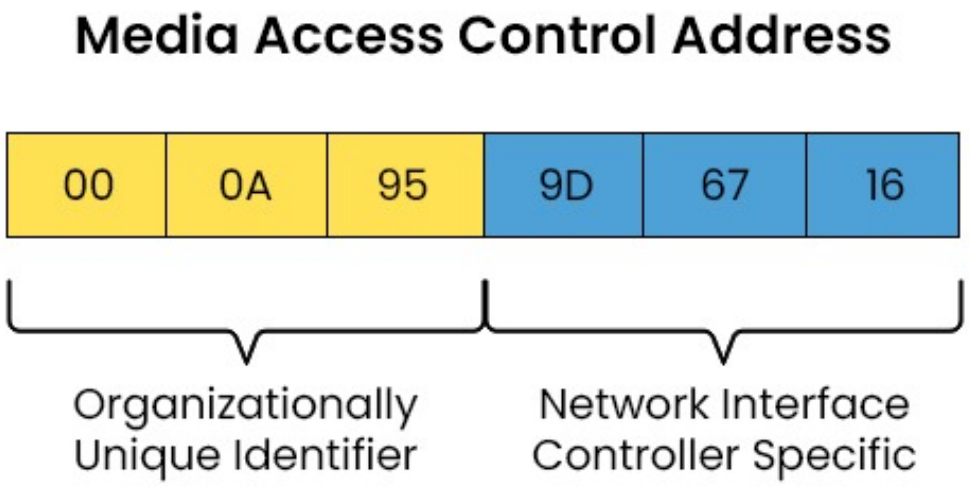

Figura 1.4: Gli indirizzi MAC sono indirizzi di 48bit, dove la prima metà rappresenta in modo univoco il produttore e la seconda metà in modo univoco la scheda di rete.[8]

I terminali mobili hanno anche un codice IMEI (*International Mobile Equipment Identity*). Questo codice numerico identifica in modo univoco un telefono cellulare oppure un modem che utilizzi la tecnologia cellulare. Viene anche usato dai telefoni satellitari. Questo rappresenta la casa produttrice e il modello del dispositivo, il luogo di costruzione o assemblaggio, il numero di serie e una cifra di controllo. Esistono anche i codici IMEISV (*IMEI Software Version*), che oltre alle informazioni riportate nel codice IMEI aggiungono le informazioni relative al *firmware* del dispositivo.

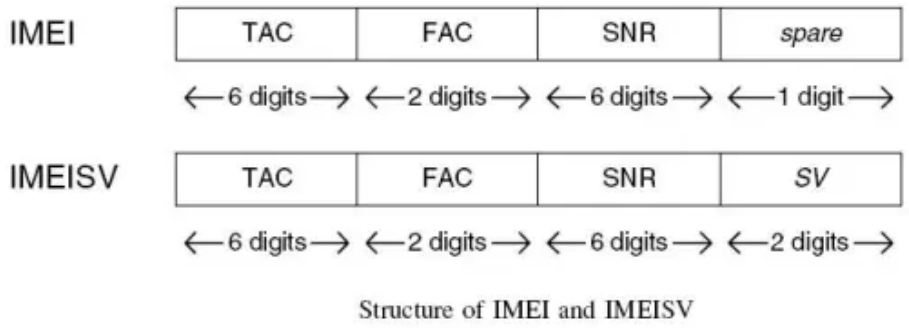

Figura 1.5: TAC (Type Approval Code); FAC (Final Assembly Code); SNR (Serial Number); SV (Software Version).[9]

Dato che questi indirizzi vengono usati per tracciare dove si trovi fisicamente un dispositivo, modificarli con una certa frequenza rende questi fondamentalmente irrintracciabili. Tuttavia la modifica di questi codici può andare contro le leggi di alcuni paesi.

1.3 Vantaggi e limiti dell'anonimato

1.3.1 Vantaggi dell'anonimato

L'anonimato online offre una serie di benefici importanti che attraggono utenti da tutto il mondo. Il primo vantaggio evidente è la protezione della *privacy*. In un'epoca in cui i dati personali sono una risorsa preziosa per le aziende e le istituzioni, la possibilità di navigare senza essere identificati permette agli utenti di mantenere il controllo su ciò che condividono. Questo controllo è cruciale per evitare che le informazioni personali vengano utilizzate in modo improprio o abusivo.

Un altro vantaggio significativo è la libertà di espressione. In contesti in cui la sorveglianza, la censura o la repressione politica sono realtà concrete, l'anonimato diventa uno strumento essenziale per poter esprimere opinioni, anche critiche, senza il timore di subire conseguenze personali. Questo non riguarda solo gli attivisti o i giornalisti, ma anche utenti comuni che desiderano discutere di temi delicati senza essere giudicati o esposti pubblicamente.

Inoltre, l'anonimato può offrire una forma di sicurezza. Persone vulnerabili, come vittime di *stalking* o minacce, o attivisti in paesi autoritari, possono utilizzare l'anonimato per proteggersi da potenziali aggressori. Nascondere la propria identità online diventa una misura di difesa indispensabile per evitare conseguenze pericolose nel mondo reale.

Infine, l'anonimato offre uno spazio per l'esplorazione personale. Molti utenti apprezzano la libertà di poter sperimentare nuove identità, di esplorare idee diverse e di partecipare a comunità online senza dover temere giudizi o aspettative legate alla propria identità reale. Questo aspetto è particolarmente rilevante nella cultura di internet, che ha sempre favorito un ambiente di creatività e sperimentazione.

1.3.2 Limiti e rischi dell'anonimato

Nonostante i vantaggi, l'anonimato *online* porta con sé anche una serie di limiti e rischi che non possono essere ignorati. Uno dei problemi principali è l'uso improprio che alcune persone fanno dell'anonimato per compiere azioni dannose. *Cyber*bullismo, *trolling*, diffusione di *fake news* e attività criminali sono solo alcuni degli esempi in cui l'anonimato permette agli autori di agire senza temere ritorsioni o punizioni. In questi casi, la mancanza di trasparenza sull'identità favorisce comportamenti irresponsabili e antisociali.

Un altro limite è legato alla responsabilità individuale. L'anonimato può ridurre il senso di responsabilità personale, poiché gli utenti sanno (o percepiscono) di non dover rispondere delle loro azioni. Questo può portare a un aumento di comportamenti negativi, come *hate speech*, minacce e truffe, che minano la qualità delle interazioni online. In assenza di un'identità associata, le conseguenze delle proprie azioni sembrano meno tangibili.

Infine, ci sono sfide anche per le autorità che cercano di applicare la legge online. L'anonimato complica il lavoro di identificazione e perseguimento di coloro che sfruttano la rete per commettere reati. Sebbene esistano tecnologie e tecniche per tracciare gli utenti, queste non sono sempre efficaci e richiedono risorse significative. Questo crea un problema di bilanciamento: proteggere il diritto all'anonimato e alla *privacy*, da una parte, e garantire la sicurezza e la giustizia, dall'altra.

Capitolo 2

Aspetti Normativi dell'Anonimato Online

Questo capitolo illustra i principali aspetti normativi che tutelano (o limitano) l'anonimato online, attraverso riferimenti legislativi nazionali e internazionali.

2.1 Anonimato nei diritti fondamentali: libertà di espressione e privacy

L'anonimato online è strettamente legato a due diritti fondamentali riconosciuti in molte democrazie: la libertà di espressione e la privacy.
La *libertà di espressione* permette agli individui di manifestare liberamente le proprie idee e opinioni, anche quando queste siano critiche o impopolari, senza il timore di subire ripercussioni o censure. In contesti in cui i governi o altri soggetti possono esercitare forme di controllo o repressione, l'anonimato diventa uno strumento chiave per garantire l'esercizio sicuro di questo diritto. Un esempio tipico è rappresentato dai paesi in cui vige una censura severa: qui, l'anonimato online consente agli utenti di esprimersi liberamente senza il rischio di essere identificati e perseguiti per le proprie opinioni politiche o sociali.

Inoltre, l'anonimato non solo protegge i dissidenti politici o gli attivisti, ma è altrettanto rilevante per le persone che desiderano discutere di argomenti sensibili in ambienti pubblici virtuali. La possibilità di nascondere la propria identità permette di creare spazi di discussione sicuri, dove gli utenti possono esprimersi senza temere di essere giudicati o stigmatizzati, o che le loro informazioni possano essere utilizzate contro di loro.

Parallelamente, il *diritto alla privacy* tutela la possibilità per ogni individuo di controllare quali informazioni personali siano rese pubbliche e come queste vengano utilizzate. Nel mondo digitale, la raccolta di dati personali è onnipresente, a partire dai dati di navigazione fino a quelli che rivelano le abitudini di consumo, la posizione geografica e le preferenze personali. Le grandi piattaforme digitali e le aziende tecnologiche traggono spesso profitto dall'analisi di questi dati, mettendo a rischio il diritto alla riservatezza. In questo contesto, l'anonimato diventa uno strumento essenziale per difendere la sfera privata dell'individuo, permettendo di accedere a servizi o interagire online senza dover necessariamente divulgare la propria identità.

La protezione legale dell'anonimato, basata sulla combinazione di libertà di espressione e privacy, varia notevolmente a seconda delle giurisdizioni. Mentre in alcune democrazie occidentali è riconosciuto come un diritto strettamente connesso alla dignità e alla libertà individuale, in altri paesi la sua applicazione è severamente limitata o addirittura proibita. Infatti in stati autoritari come Cina, Russia o Iran, l'anonimato online può essere criminalizzato o strettamente monitorato, come parte delle strategie di controllo politico. Al contrario, nelle democrazie più consolidate, vengono attuati quadri giuridici che bilanciano la necessità di proteggere l'anonimato con l'esigenza di mantenere la sicurezza e l'ordine pubblico.

Infine va sottolineato che il diritto all'anonimato, come tutti i diritti, deve essere soggetto a limitazioni e bilanciato rispetto ad altri diritti. L'anonimato può essere sfruttato per finalità illecite, come la diffusione di discorsi di odio o attività criminali, ponendo la questione di come responsabilizzare le persone per le loro azioni senza compromettere le libertà fondamentali. Tuttavia, proprio perché la libertà di espressione e il diritto alla privacy sono valori essenziali per la democrazia, l'anonimato rimane uno strumento prezioso che richiede una tutela adeguata.

2.2 L'Organizzazione delle Nazioni Unite sull'Anonimato Online

A livello internazionale, l'anonimato online trova tutela indiretta attraverso la *Dichiarazione Universale dei Diritti Umani*, adottata dalle Nazioni Unite nel 1948. In particolare, l'articolo 19 sancisce il diritto alla libertà di espressione, affermando che "ogni individuo ha il diritto alla libertà di opinione e di espressione; incluso il diritto di non essere molestato per le proprie opinioni

e di cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e indipendentemente dalle frontiere"[10] principio, pur non menzionando esplicitamente l'anonimato, è interpretato come una protezione implicita dello stesso, poiché l'anonimato rappresenta un mezzo cruciale per consentire alle persone di esprimersi liberamente in contesti in cui potrebbero altrimenti essere soggette a ritorsioni o censura. Questo articolo, quindi, descrive come il diritto all'anonimato online può essere visto come una delle modalità pratiche attraverso cui si realizza il diritto più ampio alla libertà di espressione.

Oltre alla Dichiarazione Universale dei Diritti Umani, negli ultimi decenni le Nazioni Unite hanno rafforzato la tutela della privacy e dell'anonimato online attraverso una serie di risoluzioni e rapporti dedicati alla protezione dei diritti digitali. Uno dei documenti più rilevanti è la *Risoluzione dell'Assemblea Generale delle Nazioni Unite A/RES/68/167 del 2013*, intitolata "Il diritto alla privacy nell'era digitale", che ha riconosciuto per la prima volta la centralità della protezione della privacy nei contesti digitali[11]. La risoluzione esorta gli Stati membri a rispettare e garantire il diritto alla privacy online, sottolineando l'importanza di sviluppare normative che proteggano i cittadini dall'accesso illegittimo ai propri dati personali. Questa risoluzione rappresenta un passaggio fondamentale nel riconoscimento del diritto alla privacy digitale come componente integrante dei diritti umani.

Un ulteriore passo avanti è stato compiuto con la *Risoluzione A/HRC/-RES/32/13 del 2016*, adottata dal Consiglio per i Diritti Umani delle Nazioni Unite. Questa risoluzione riafferma che gli stessi diritti che le persone hanno offline devono essere protetti anche online, inclusi il diritto alla privacy e la libertà di espressione[12]. In questo contesto l'anonimato online emerge come uno strumento per garantire tali diritti nel mondo digitale. La risoluzione sottolinea che le misure di sorveglianza o restrizione della privacy devono essere conformi alle leggi internazionali sui diritti umani e devono rispettare i principi di necessità e proporzionalità.

L'implementazione pratica delle normative internazionali sull'anonimato varia notevolmente tra i diversi paesi. Ad esempio, paesi come la Germania e i Paesi Bassi offrono un alto livello di protezione della privacy e dell'anonimato online, anche per i whistleblower e gli attivisti che si avvalgono di tecnologie per nascondere la propria identità. Al contrario, altre nazioni, come la Cina e l'Arabia Saudita, applicano severe restrizioni all'uso dell'anonimato online, giustificandole con motivazioni legate alla sicurezza nazionale e alla necessità di mantenere il controllo politico. In Cina, ad esempio, la normativa impone l'obbligo di registrare le informazioni personali degli utenti presso i fornitori di

servizi internet, rendendo di fatto impossibile l'anonimato completo. Questo approccio resta in netto contrasto con gli standard promossi dalle Nazioni Unite, evidenziando il divario tra i principi internazionali e le pratiche locali.

Un caso emblematico di tale discrepanza è la Russia, dove, nonostante la firma di trattati internazionali sui diritti umani, sono state introdotte leggi che limitano fortemente l'anonimato online, come la cosiddetta legge *Yarovaya* (2016), che impone ai fornitori di servizi internet di conservare i dati degli utenti per almeno sei mesi e li obbliga a fornire le informazioni alle autorità su richiesta[13]. Questi esempi mostrano come l'implementazione delle norme internazionali possa incontrare difficoltà nei contesti nazionali autoritari, dove possono entrare in gioco considerazioni legate alla sicurezza nazionale o al controllo della popolazione.

In definitiva, sebbene le Nazioni Unite e altri organismi internazionali abbiano adottato misure importanti per la tutela dell'anonimato online, l'efficacia di queste normative dipende in gran parte dalla volontà politica dei singoli Stati e dal loro grado di conformità ai principi internazionali sui diritti umani. Ciò crea un panorama frammentato in cui, mentre alcuni paesi promuovono attivamente l'anonimato come diritto fondamentale, altri ne limitano l'uso per ragioni di controllo e sicurezza.

2.3 Norme Europee sull'Anonimato Online

L'Unione Europea ha sviluppato un quadro normativo tra i più avanzati al mondo per la tutela della privacy e, di conseguenza, per la protezione dell'anonimato online. Questo approccio trova fondamento nella *Carta dei diritti fondamentali dell'Unione Europea*, un documento che stabilisce i principi fondamentali sui quali si basano le normative europee in materia di diritti digitali. In particolare, l'articolo 8 della Carta riconosce esplicitamente il diritto alla protezione dei dati personali[14], mentre l'articolo 11 sancisce il diritto alla libertà di espressione[15]. Questi due articoli, letti insieme, creano un quadro giuridico che tutela non solo la privacy degli utenti, ma anche l'anonimato, permettendo agli individui di esprimersi liberamente senza il timore di essere tracciati o identificati . In un mondo in cui i dati personali sono sempre più esposti e oggetto di sorveglianza, l'Unione Europea si impegna a difendere l'anonimato come un elemento cruciale per la protezione della sfera privata.

Un ruolo centrale nella protezione della privacy e dei diritti digitali è svolto dal *Regolamento Generale sulla Protezione dei Dati (GDPR)*, entrato in vigore nel 2018. Il GDPR è considerato una pietra miliare nella regolamentazione dei dati personali a livello globale e ha stabilito standard molto rigorosi per il trattamento delle informazioni personali da parte delle aziende, sia all'interno che al di fuori dell'Unione Europea. Tra i principi chiave del GDPR troviamo il concetto di "data minimization" (minimizzazione dei dati), che incoraggia le organizzazioni a raccogliere solo le informazioni strettamente necessarie e a trattarle in modo tale da ridurre al minimo i rischi di violazione della privacy[16]. Pur non menzionando espressamente l'anonimato, il GDPR offre strumenti legali che possono essere utilizzati per garantirlo, come il diritto alla cancellazione (noto anche come "diritto all'oblio") e il diritto alla limitazione del trattamento . Queste disposizioni permettono agli utenti di richiedere la rimozione dei propri dati o di limitarne l'utilizzo, contribuendo in modo significativo alla salvaguardia della riservatezza online.

La *Direttiva ePrivacy*, spesso considerata un complemento del GDPR, gioca un ruolo cruciale nella protezione delle comunicazioni elettroniche. Questa direttiva, che disciplina specificamente la riservatezza delle comunicazioni via email, messaggi e altri servizi digitali, include una serie di disposizioni che mirano a garantire la confidenzialità delle comunicazioni elettroniche e, indirettamente, l'anonimato degli utenti durante la navigazione e l'uso di servizi online[17]. La revisione di questa direttiva, attualmente in discussione nelle istituzioni europee, mira a rafforzare ulteriormente queste tutele, introducendo nuove regole per i servizi di messaggistica istantanea e i servizi di comunicazione over-the-top (OTT), come WhatsApp o Telegram, ampliando così la portata delle normative in materia di privacy digitale.

La giurisprudenza della *Corte Europea dei Diritti dell'Uomo (CEDU)* ha anch'essa avuto un ruolo significativo nella definizione dei confini tra anonimato, privacy e libertà di espressione. In diverse sentenze, la Corte ha sottolineato l'importanza di proteggere la libertà di espressione online, anche quando questa viene esercitata in forma anonima, riconoscendo che in molti casi l'anonimato è essenziale per tutelare i diritti individuali in contesti di censura o repressione politica. Ad esempio, in casi come *K.U. contro Finlandia* (2008), la CEDU ha ribadito la necessità di bilanciare il diritto alla privacy con la libertà di espressione e la protezione dei minori, evidenziando come l'anonimato non possa essere garantito in maniera assoluta, ma debba essere contemperato con altre esigenze di tutela collettiva[18].

In sintesi, l'Unione Europea si distingue per il suo approccio complesso e ar-

ticolato alla protezione dell'anonimato online, bilanciando il diritto alla privacy con altre esigenze di sicurezza e trasparenza. Il quadro normativo europeo, che si basa su documenti fondamentali come la Carta dei diritti fondamentali, il GDPR e la Direttiva ePrivacy, non solo riconosce l'importanza dell'anonimato come strumento per la protezione dei diritti individuali, ma cerca anche di adattarsi ai rapidi cambiamenti del mondo digitale, promuovendo normative sempre più avanzate per affrontare le nuove sfide legate alla privacy e alla sicurezza online.

2.4 Norme Italiane sull'Anonimato Online

In Italia, l'anonimato online è tutelato principalmente attraverso due pilastri normativi: la Costituzione Italiana e il Codice della Privacy. L'*articolo 21 della Costituzione Italiana* garantisce a ogni cittadino il diritto di esprimere liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione, un principio che si applica tanto ai media tradizionali quanto alle piattaforme digitali [19]. Sebbene il testo costituzionale non menzioni esplicitamente l'anonimato, la libertà di espressione può essere interpretata come una tutela implicita del diritto di manifestare le proprie opinioni anche in maniera anonima, specialmente in contesti in cui l'identificazione dell'individuo potrebbe comportare rischi per la sua sicurezza o il suo benessere. In questo senso, l'anonimato diventa uno strumento essenziale per proteggere l'individuo in situazioni delicate, come quelle relative alla dissidenza politica, alla critica sociale, o alla denuncia di pratiche illecite.

Accanto alla Costituzione, il *Codice della Privacy* (Decreto Legislativo 30 giugno 2003, n. 196, modificato dal Decreto Legislativo 101/2018 per l'adeguamento al GDPR), rappresenta un quadro legislativo chiave per la protezione dei dati personali in Italia[20]. Questo codice stabilisce regole rigide per il trattamento dei dati personali, imponendo a chi raccoglie, tratta o conserva informazioni sui cittadini italiani di rispettare una serie di obblighi volti a salvaguardare la riservatezza. Uno degli aspetti centrali del Codice è la concessione agli individui di diritti specifici, come il diritto di accedere ai propri dati, di rettificarli, cancellarli o limitarne il trattamento, tutti strumenti che possono essere utilizzati per ottenere o mantenere l'anonimato online. Questo è particolarmente importante in un'epoca in cui le informazioni personali possono essere sfruttate per profilare e tracciare gli utenti senza il loro consenso esplicito.

Un altro attore fondamentale nella tutela della privacy e dell'anonimato online in Italia è l'*Autorità Garante per la Protezione dei Dati Personali*, un organismo indipendente che ha il compito di vigilare sull'applicazione del Codice della Privacy e di altre leggi rilevanti, nonché di emettere linee guida e decisioni in merito alla protezione dei dati. Il Garante ha affrontato numerosi casi che coinvolgono questioni di privacy digitale, inclusi quelli legati all'anonimato, e ha ribadito in più occasioni che la protezione dei dati personali è un diritto fondamentale, soprattutto in un contesto digitale in cui le informazioni possono essere diffuse rapidamente e senza il controllo dell'utente. Le decisioni del Garante si basano spesso sulla necessità di bilanciare la tutela della privacy e dell'anonimato con altri interessi, come la sicurezza pubblica e la libertà di informazione.

La giurisprudenza italiana ha inoltre riconosciuto l'importanza dell'anonimato in contesti specifici, come la libertà di stampa e la tutela degli informatori (whistleblowers). In alcuni casi, i tribunali italiani hanno stabilito che l'anonimato è un elemento essenziale per proteggere coloro che denunciano illeciti o che offrono informazioni sensibili, poiché la rivelazione della loro identità potrebbe esporli a ritorsioni. Ad esempio, nel contesto delle inchieste giornalistiche o nelle cause che coinvolgono whistleblowers, la tutela dell'anonimato è stata considerata fondamentale per garantire che queste persone possano agire senza timori di ritorsioni.

Detto questo, l'anonimato non è garantito in maniera assoluta in Italia. Esistono restrizioni significative in determinate circostanze, per motivi legati alla sicurezza nazionale e al contrasto del crimine. Ad esempio, nell'ambito delle indagini giudiziarie o nella lotta al terrorismo e alla criminalità organizzata, le forze dell'ordine hanno il potere di identificare gli individui, anche online, quando ciò sia ritenuto necessario per prevenire attività criminali o proteggere la sicurezza pubblica. Queste limitazioni sono state giustificate dal legislatore italiano come misure indispensabili per prevenire l'abuso dell'anonimato a scopi illeciti, mantenendo un equilibrio tra la tutela dei diritti individuali e la protezione degli interessi collettivi.

2.5 Confronto tra Anonimato nella Vita Reale e Online

Il confronto tra anonimato nella vita reale e online mette in luce differenze significative, soprattutto dal punto di vista normativo. Nella vita reale, l'anonimato è garantito da strumenti giuridici consolidati. Un esempio lampante è il

diritto di voto segreto, che è tutelato per evitare ritorsioni o pressioni sull'elettore. Questa forma di anonimato è ben radicata nei sistemi democratici e sancita da normative come l'articolo 48 della Costituzione Italiana. Altri esempi includono la possibilità di usare pseudonimi in ambito artistico o letterario, o la partecipazione anonima a manifestazioni pubbliche, il cui diritto è riconosciuto da normative che garantiscono la libertà di riunione e di espressione senza l'obbligo di identificazione.

Nel contesto online, tuttavia, l'anonimato è regolamentato in modo diverso e presenta sfide più complesse. L'architettura stessa delle tecnologie digitali genera tracce identificative (ad esempio indirizzi IP, cookies e metadati) che rendono l'anonimato tecnicamente più difficile da mantenere. Le normative in ambito digitale, come il GDPR, si concentrano principalmente sulla protezione dei dati personali, permettendo agli individui di esercitare diritti come quello alla cancellazione e all'accesso ai propri dati. Tuttavia, la stessa normativa non garantisce esplicitamente l'anonimato in tutti i contesti, soprattutto in presenza di esigenze legate alla sicurezza pubblica o alla prevenzione di reati.

Un'importante distinzione da considerare è che, mentre nella vita reale l'anonimato non richiede grandi accortezze che sono invece necessarie per mantenere l'anonimato online. Sono infatti necessari strumenti tecnici più sofisticati, come l'uso di reti private virtuali (VPN), crittografia o software di navigazione anonima (ad esempio Tor). A livello giuridico, l'identificazione online è spesso richiesta in circostanze specifiche, come nella registrazione su piattaforme di social media o per l'accesso a servizi governativi, a seconda delle leggi nazionali. In alcuni paesi, come la Corea del Sud, esistono leggi che impongono l'uso del nome reale per l'accesso a determinati servizi online, mentre in Europa, il GDPR fornisce una maggiore flessibilità nell'uso di pseudonimi.

In conclusione, mentre l'anonimato nella vita reale è spesso garantito da una struttura normativa più chiara e diretta, nell'ambiente digitale le normative sono più frammentarie e, per garantirlo, è necessario un uso consapevole di strumenti tecnologici. Il quadro giuridico europeo, pur riconoscendo l'importanza della privacy e dei dati personali, non offre una tutela piena e uniforme per l'anonimato online, lasciando spazio a deroghe significative in nome della sicurezza e della protezione contro crimini informatici.

2.6 Sfide Tecniche e Legali dell'Anonimato Online

Garantire l'anonimato online comporta numerose sfide, sia tecniche che legali, che spesso si intrecciano a causa della natura globale di Internet e della diversità delle normative nazionali. Dal punto di vista tecnico, una delle principali difficoltà è che la rete Internet è stata originariamente progettata per garantire l'efficienza nella trasmissione dei dati piuttosto che la privacy o l'anonimato degli utenti. I protocolli che regolano le comunicazioni digitali, come il protocollo IP (Internet Protocol), richiedono che ogni dispositivo collegato alla rete venga identificato da un indirizzo IP unico, rendendo più difficile l'anonimato. Anche l'uso diffuso di cookies e tracker da parte delle piattaforme web contribuisce a rendere complesso mantenere l'anonimato online, poiché questi strumenti sono progettati per monitorare il comportamento dell'utente a scopo di profilazione e pubblicità.

Strumenti come Tor (The Onion Router), VPN (Virtual Private Networks)che abbiamo analizzato precedentemente rappresentano i principali mezzi tecnologici per nascondere l'identità e la posizione dell'utente, ma questi strumenti non sono infallibili. Tor, ad esempio, pur essendo uno dei metodi più sicuri per garantire l'anonimato, non è immune da vulnerabilità, come gli attacchi di correlazione del traffico che possono essere utilizzati da attori statali o da organizzazioni con risorse sufficienti per monitorare contemporaneamente più punti della rete. Inoltre, le VPN, pur offrendo una buona protezione contro la sorveglianza di massa, richiedono agli utenti di fidarsi dei fornitori di tali servizi, che potrebbero essere soggetti a richieste di dati da parte delle autorità governative o potrebbero essere compromessi da attacchi informatici.

Dal punto di vista legale, le sfide sono forse ancora più complesse. Internet è uno spazio globale, ma le leggi che regolano l'anonimato e la privacy online variano notevolmente da una giurisdizione all'altra. Ad esempio, l'Unione Europea, con il GDPR (Regolamento Generale sulla Protezione dei Dati), offre una protezione piuttosto rigorosa dei dati personali, anche se non menziona esplicitamente il diritto all'anonimato. Tuttavia, altri paesi, come la Cina e la Russia, impongono forti restrizioni sull'uso dell'anonimato online per motivi di sicurezza nazionale, richiedendo la registrazione con il nome reale per accedere a determinati servizi o bloccare completamente l'uso di VPN o strumenti come Tor disomogeneità normativa crea problemi di giurisdizione. Un utente che tenta di mantenere l'anonimato potrebbe navigare su un sito ospitato in un paese con normative più permissive in termini di privacy, ma essere soggetto alle leggi di un altro paese che richiede l'identificazione obbligatoria degli utenti

online. Questo genera una serie di incertezze legali, complicando il lavoro delle autorità che cercano di applicare la legge e la protezione della privacy a livello transnazionale. Un esempio di questa complessità è rappresentato dal caso *Google Spain v. AEPD* (2014)[21], che ha sollevato la questione dell'equilibrio tra il diritto alla privacy e il diritto all'informazione nel contesto della rete.

Un'altra sfida legale cruciale riguarda il bilanciamento tra anonimato e sicurezza pubblica. L'anonimato online è spesso visto con sospetto dai governi e dalle forze dell'ordine, in quanto può essere sfruttato per attività criminali, come diffamazione, la diffusione di contenuti estremisti o vietati e l'organizzazione di attacchi informatici. In risposta, molti stati adottano leggi che limitano l'anonimato, soprattutto per motivi di sicurezza nazionale o di contrasto al terrorismo. Un esempio è la normativa statunitense che, nel quadro del *Patriot Act*, ha ampliato i poteri delle agenzie di intelligence per monitorare le attività online, includendo la possibilità di richiedere dati sensibili alle aziende tecnologiche.

Tuttavia, tali restrizioni sollevano questioni etiche e giuridiche riguardanti il diritto alla privacy e alla libertà di espressione, sanciti da molte costituzioni e trattati internazionali, come la Dichiarazione Universale dei Diritti Umani e la Carta dei diritti fondamentali dell'Unione Europea. Il rischio è che, in nome della sicurezza, si limiti eccessivamente la libertà individuale, rendendo difficile per giornalisti, attivisti o dissidenti politici esprimersi liberamente senza timore di ritorsioni. A questo si aggiunge la difficoltà di sviluppare una regolamentazione uniforme che bilanci i diritti individuali e le esigenze di sicurezza in un contesto digitale che non conosce confini geografici.

In conclusione, le sfide tecniche e legali legate all'anonimato online sono profonde e da affrontare su più livelli. Da un lato, i progressi tecnologici continuano a offrire nuovi strumenti per proteggere la privacy, ma allo stesso tempo, le infrastrutture digitali esistenti e le normative divergenti a livello globale complicano ulteriormente la protezione dell'anonimato. Questo richiede un approccio equilibrato che tenga conto della tutela dei diritti individuali senza compromettere la sicurezza collettiva.

2.7 Sintesi e Riflessioni Finali

In questo capitolo abbiamo esplorato i diversi aspetti normativi che influenzano l'anonimato online, sia a livello internazionale che nazionale. Mentre le normative internazionali, europee e italiane offrono un quadro giuridico solido per proteggere l'anonimato, restano molte sfide, soprattutto a causa della natu-

ra globale e decentralizzata di Internet. Le differenze giuridiche tra i vari paesi complicano ulteriormente la situazione, creando disparità nell'applicazione delle leggi.

L'anonimato, dunque, è un diritto strettamente legato alla libertà di espressione e alla privacy, ma che richiede un bilanciamento costante con la sicurezza e la protezione degli interessi collettivi. Nel futuro, sarà necessario sviluppare soluzioni innovative, sia tecniche che giuridiche, per garantire che l'anonimato possa essere tutelato in un contesto digitale sempre più complesso.

Capitolo 3

Contratti di Utilizzo dei Social Network e l'Anonimato Online: Tendenze e Contraddizioni

3.1 Importanza dei Contratti di Utilizzo nei Social Media

I contratti di utilizzo, noti anche come termini di servizio o ToS (Terms of Service), sono documenti legali fondamentali che disciplinano l'interazione degli utenti con le piattaforme social. Questi contratti definiscono diritti e doveri sia per gli utenti che per le piattaforme, stabilendo un quadro normativo per l'uso dei servizi. La loro importanza è accentuata dall'ampia diffusione dei social media, che rappresentano una parte significativa della comunicazione contemporanea. Secondo l'*Organizzazione per la Cooperazione e lo Sviluppo Economico* (OCSE), nel 2019, oltre il 60% della popolazione mondiale utilizza i social media[22], sottolineando così il bisogno di normative chiare e trasparenti.

I contratti di utilizzo fungono da strumenti di protezione per entrambe le parti. Da un lato, forniscono alle piattaforme una base legale per moderare i contenuti, proteggere i propri interessi commerciali e garantire un ambiente sicuro. Dall'altro, informano gli utenti sui propri diritti, inclusi quelli relativi alla privacy e alla gestione dei dati personali. Secondo il GDPR (Regolamento Generale sulla Protezione dei Dati), le piattaforme sono obbligate a informare gli utenti in modo chiaro e comprensibile riguardo all'uso dei loro dati, evidenziando la necessità di contratti di utilizzo che rispettino le normative europee[16].

Tuttavia, la complessità e la lunghezza di questi contratti spesso portano gli

utenti a non leggerli attentamente, comportando una mancanza di consapevolezza riguardo ai termini a cui acconsentono. Secondo uno studio condotto dalla Stanford University, il 91% degli utenti non legge mai i contratti di servizio, il che solleva preoccupazioni su come le clausole inique possano influenzare la libertà di espressione e la protezione della privacy[23]. Questo evidenzia l'importanza di una maggiore trasparenza e accessibilità nei contratti di utilizzo, per garantire che gli utenti possano prendere decisioni informate riguardo al proprio coinvolgimento nelle piattaforme social.

3.2 Panoramica delle piattaforme: Meta (Facebook/Instagram), X (Twitter) e TikTok

Meta, X (ex Twitter) e TikTok sono i tra i social network più diffusi e si distinguono nettamente per il tipo di contenuti proposti e per l'audience che attraggono, sia in termini di età che di distribuzione geografica. Facebook e Instagram di Meta sono tra le piattaforme più globali e diversificate per fascia d'età, ma con una tendenza all'utilizzo maggiore da parte degli utenti sopra i 25 anni, in particolare su Facebook[24]. Instagram, invece, mantiene un appeal più alto tra i giovani, specie quelli tra i 18 e i 34 anni[25], grazie alla sua natura visiva e all'orientamento verso immagini e video brevi.

X (denominato precedentemente Twitter) è conosciuto per il suo approccio centrato sulle notizie e sui contenuti testuali, con una base di utenti altamente concentrata negli Stati Uniti, Europa e in Giappone[26]. A livello di distribuzione dell'età, X è popolare tra i giovani adulti[27], sebbene stia cercando di espandere la propria portata con contenuti più multimediali e nuove funzionalità per attirare nuove fascie anagrafiche. La sua natura come piattaforma di dibattito e aggiornamento in tempo reale la rende ideale per la rapida diffusione di notizie e discussioni politiche.

Infine, TikTok è ampiamente riconosciuto come la piattaforma preferita della Gen Z e Gen Alpha, con il 60% degli utenti sotto i 25 anni[28][29] e una forte base di utenti negli Stati Uniti, in Sud America, in Europa e nel Sud-est asiatico[30]. Il suo formato di video brevi e targettizzati grazie ad algoritmi avanzati ha permesso una rapida espansione globale. TikTok si differenzia anche per la forte spinta verso la localizzazione dei contenuti, adattando trend e feed alle specificità culturali e alle preferenze locali.

Queste differenze nel target e nella fruizione dei contenuti influenzano il modo in cui ogni piattaforma sviluppa le proprie politiche di moderazione, privacy e distribuzione, rendendo complesso il confronto diretto in termini di regolamentazione e impatto sugli utenti.

3.3 Definizione e scopo dei contratti di utilizzo

I contratti di utilizzo o termini di servizio (ToS) sono un accordo legale tra un fornitore di servizi e un utente del servizio. Il servizio può essere un sito web, un'applicazione o un altro software. In genere, l'utente deve accettare i ToS prima di poter accedere al servizio.

In primo luogo, i ToS proteggono il fornitore di servizi e il servizio da abusi o furti da parte degli utenti. Tuttavia, questi termini possono anche includere clausole che concedono il permesso dell'utente al fornitore del servizio di svolgere altre attività.

Altri nomi per questo tipo di accordo sono "termini d'uso" e "termini e condizioni". L'accettazione dei ToS da parte dell'utente può essere esplicita, come la spunta di una casella "Accetto...", o implicita, come la frase "Utilizzando questo sito web si accetta..." su un sito web. I ToS sono legalmente vincolanti sia per il fornitore del servizio che per l'utente. Tuttavia, questi termini sono spesso lunghi e scritti in un gergo legale denso e prolisso e anche a causa di ciò gli utenti raramente leggono i termini prima di accettare[23].

I contratti di utilizzo appaiono in molte situazioni, come l'installazione di un software o di un'applicazione, l'iscrizione a un servizio o l'utilizzo di un sito web. Online, i ToS sono comuni nei luoghi in cui l'utente e il sito web interagiscono (come l'e-commerce) o in tutto ciò che comporta un account sicuro (come i social media).

I termini d'uso specificano quali servizi vengono forniti e le regole che si applicano all'utente. Specificano ciò che l'utente può o non può fare durante l'utilizzo di un servizio (ad esempio, definiscono quali comportamenti non sono consentiti sui social media). I ToS solitamente includono clausole che proteggono la proprietà intellettuale del fornitore (come loghi e contenuti) dall'uso illecito o dal furto da parte dell'utente. La proprità intellettuale è riconosciuta a livello internazionale, attraverso vari trattati e accordi, come quelli promossi dall'Organizzazione Mondiale della Proprità Intellettuale (WIPO). Ad ogni modo ogni paese ha le proprie leggi nazionali che regolano la protezione della

proprietà intellettuale, che quindi rimane valida anche se non citata direttamente nei ToS. Se applicabili, vengono trattati anche i termini di pagamento, come le tariffe di abbonamento, i rinnovi automatici e le politiche di cancellazione.

I contratti di utilizzo descrivono anche le protezioni che il fornitore di servizi si riserva. Un fornitore di servizi può indicare le circostanze in cui può sospendere o chiudere un account. Idealmente ciò avverrebbe solo se un utente violasse i ToS, ma alcune aziende o siti web si riservano il diritto di sospendere o chiudere l'account per qualsiasi motivo. Un'altra protezione comune è la limitazione della responsabilità. In questo caso, l'accordo stabilisce anche che il provider non può essere ritenuto responsabile per il comportamento illecito degli utenti.

Il provider può anche rilasciare un'informativa sulla privacy. A seconda della natura del servizio, un'informativa sulla privacy può essere richiesta dalla legge. Il suo scopo è quello di informare e proteggere l'utente in merito al trattamento legale dei suoi dati e in alcuni casi deve essere accettata esplicitamente. Nella maggior parte dei casi, tuttavia, i termini di servizio non sono obbligatori per legge. L'adozione spetta al fornitore e si concentrano sulla tutela del fornitore stesso.

In genere, un'informativa sulla privacy riguarda i dati che possono essere raccolti, le modalità (e la durata) di conservazione e le modalità di utilizzo dei dati da parte del fornitore di servizi, sia nell'ambito della fornitura del servizio che per altri fini, ad esempio pubblicitari. Un'informativa sulla privacy riguarderà anche i soggetti con cui il fornitore può condividere i dati raccolti.

I termini d'uso sono più generali e coprono più aree del solo trattamento dei dati. Se il servizio prevede il trattamento dei dati, i ToS possono includere i contenuti solitamente presenti in un'informativa sulla privacy, oppure possono semplicemente rimandare a un documento separato sull'informativa sulla privacy.

3.4 Impatti legali dei contratti di utilizzo

I contratti di utilizzo delle piattaforme social, come quelli di Meta, X e TikTok, hanno implicazioni legali significative per gli utenti e per le aziende che li gestiscono. A livello giuridico, questi contratti rappresentano accordi vincolanti che stabiliscono i diritti e le responsabilità di entrambe le parti. Gli utenti, accettando i termini, concedono alle piattaforme una serie di autorizza-

zioni, tra cui l'uso dei dati personali e dei contenuti generati, mentre le aziende definiscono le proprie responsabilità riguardo alla sicurezza, alla moderazione dei contenuti e alla gestione della privacy.

Dal punto di vista degli utenti, le piattaforme tendono a limitare la propria responsabilità per eventuali danni derivanti dall'uso dei loro servizi. Queste clausole, spesso inserite nei termini di servizio, mirano a proteggere le aziende da possibili cause legali, riducendo al minimo i rischi associati alla gestione di contenuti pubblicati dagli utenti. Tuttavia, tali clausole possono lasciare gli utenti vulnerabili, poiché le piattaforme non sono obbligate a rispondere per le conseguenze delle interazioni tra utenti o per i danni causati da contenuti inappropriati o diffamatori.

Per quanto riguarda la protezione dei dati, normative come il GDPR (Regolamento Generale sulla Protezione dei Dati) hanno imposto obblighi specifici alle piattaforme che operano nell'Unione Europea, richiedendo una maggiore trasparenza e il consenso esplicito degli utenti per la raccolta e il trattamento dei dati. Le piattaforme sono legalmente obbligate a permettere agli utenti di esercitare il diritto di accesso, rettifica e cancellazione dei propri dati personali, ma la complessità e la lunghezza dei contratti rendono spesso difficile per gli utenti comprendere appieno queste possibilità. Inoltre la direttiva ePrivacy[17] regola le modalità con cui sia possibile raccogliere i dati degli utenti tramite i cookies. La direttiva impone che l'utente esprima il suo consenso per essere tracciato dai cookies non essenziali al funzinamento del sito. Accettando tutti i cookies si accettando svariati (talvolta centinaia) cookies di terze parti, spesso per finalità di marketing.

Infine, i contratti di utilizzo sollevano questioni etiche e legali legate alla proprietà intellettuale. Spesso le piattaforme richiedono licenze globali e trasferibili sui contenuti creati dagli utenti, permettendo alle aziende di utilizzare e persino monetizzare questi contenuti senza dover corrispondere royalties o compensazioni. Questo aspetto può suscitare controversie, poiché gli utenti potrebbero non essere consapevoli delle implicazioni di tali licenze.

3.5 Questioni etiche legate alla gestione dei dati e alla moderazione dei contenuti

La gestione dei dati personali e la moderazione dei contenuti nelle piattaforme social pongono numerosi dilemmi etici, in quanto influenzano direttamente i diritti fondamentali degli utenti, come la privacy, la libertà di espressione

e la sicurezza online. Le piattaforme, come Meta, X e TikTok, si trovano costantemente a bilanciare il rispetto della privacy degli utenti con l'esigenza di garantire un ambiente sicuro e conforme alle normative nazionali e internazionali.

Inoltre le piattaforme non sono tenute a tutelare l'utenza dai crimini informatici, tra i più diffusi la diffamazione, la sostituzione di persona o l'incitamento all'odio. Le piattaforme permettono agli utenti di segnalare eventuali comportamenti scorretti da parte degli utenti per poi eventualmente prendere azioni nei confronti dei contenuti o degli utenti lesivi.

3.5.1 Gestione dei Dati Personali e Privacy

La raccolta e l'elaborazione dei dati personali sono aspetti centrali delle attività delle piattaforme social, le quali spesso monetizzano i dati degli utenti attraverso la personalizzazione delle pubblicità. Secondo le disposizioni del GDPR e di altre normative internazionali sulla privacy, le piattaforme sono tenute a informare chiaramente gli utenti riguardo al trattamento dei loro dati e a garantire il diritto di accesso, rettifica e cancellazione. Tuttavia, la trasparenza su come i dati sono utilizzati, specialmente in riferimento alla condivisione con terze parti o all'elaborazione tramite algoritmi di machine learning, è spesso limitata e difficile da comprendere per gli utenti, lasciando margini di ambiguità su possibili utilizzi indebiti o non autorizzati dei dati.

Le piattaforme devono anche garantire che le informazioni raccolte siano protette da eventuali violazioni, ma incidenti significativi, come quello subito da Facebook nel 2019[31], mostrano come la sicurezza dei dati sia un obiettivo ancora difficile da raggiungere e mantenga un livello di rischio elevato per gli utenti. La vulnerabilità dei dati personali rappresenta quindi un problema etico importante, poiché una gestione non adeguata potrebbe compromettere la fiducia degli utenti e causare danni irreversibili alla loro reputazione e sicurezza personale.

In aggiunta, il principio contenuto nell'*articolo 51 del Codice Penale* italiano stabilisce che l'esercizio di un diritto o l'adempimento di un dovere imposto da una norma giuridica o da un ordine legittimo della pubblica autorità esclude la punibilità[32]. Questo principio, applicato al contesto delle piattaforme social e al trattamento dei dati, introduce una riflessione sull'equilibrio tra il diritto degli utenti alla protezione dei dati personali e gli obblighi che le piattaforme potrebbero avere nel caso in cui ricevano ordini di divulgazione o trattamento dei dati da parte delle autorità. Tale scenario sottolinea come, se un operatore segue un ordine legittimo, anche quando esso comporta un rischio per la privacy dell'utente, può non essere ritenuto responsabile penalmente; al contrario,

un'eventuale esecuzione di un ordine illegittimo potrebbe portare a conseguenze legali per l'operatore stesso. Questo aspetto evidenzia la complessità della gestione dei dati e dei diritti degli utenti, soprattutto quando in gioco sono interessi pubblici di sicurezza e giustizia.

3.5.2 Moderazione dei Contenuti e Libertà di Espressione

La moderazione dei contenuti rappresenta un tema complesso e controverso, poiché le piattaforme digitali devono trovare un equilibrio tra la libertà di espressione degli utenti e la necessità di prevenire la diffusione di contenuti dannosi, come incitamento all'odio, disinformazione e violenza. Tuttavia, ogni piattaforma adotta politiche di moderazione differenti. Ad esempio, TikTok si distingue per un approccio rigoroso nel rimuovere contenuti non conformi alle sue regole, per preservare un ambiente sicuro, specie per gli utenti più giovani. Al contrario, X ha storicamente favorito una maggiore libertà di espressione, ma è sottoposto a crescenti pressioni per limitare i contenuti estremisti e le fake news. Meta, che gestisce Facebook e Instagram, adotta una strategia intermedia, combinando algoritmi e revisori umani per monitorare i contenuti in contesti delicati come la disinformazione su salute pubblica ed elezioni.

La crescente adozione di algoritmi di intelligenza artificiale per identificare contenuti violenti o ingannevoli solleva però preoccupazioni etiche: tali algoritmi possono involontariamente censurare espressioni lecite o discriminare gruppi specifici. Inoltre, l'applicazione discrezionale delle politiche di moderazione genera incertezza negli utenti, che non possono prevedere con certezza quali contenuti possano essere rimossi. Questa mancanza di trasparenza rischia di influenzare negativamente il dibattito pubblico e compromettere il diritto all'informazione.

3.5.3 Controllo delle Piattaforme e Autonomia degli Utenti

Il controllo esercitato dalle piattaforme sui contenuti degli utenti introduce una dinamica di potere che limita l'autonomia degli stessi. Sebbene gli utenti creino contenuti, la visibilità e la distribuzione degli stessi è spesso determinata dalle piattaforme, che possono limitarne l'accesso se violano le loro linee guida. Tuttavia, il funzionamento degli algoritmi che selezionano i contenuti rimane poco trasparente, generando una percezione di arbitrio che può sembrare influenzata da pressioni politiche o commerciali. Questo controllo quasi esclusivo solleva domande sull'equità del processo di moderazione e sulla possibilità di censure non dichiarate, che minerebbero la neutralità del servizio e la diversità di opinioni.

3.6 Responsabilità delle piattaforme e degli utenti

Le responsabilità di piattaforme come Meta, X e TikTok, così come quelle degli utenti, variano notevolmente in base ai termini di utilizzo e alle leggi applicabili. Le piattaforme, in qualità di intermediari digitali, devono bilanciare l'obiettivo di favorire la comunicazione e l'espressione personale con l'obbligo di garantire un ambiente sicuro, moderare i contenuti inappropriati e proteggere la privacy degli utenti. Tuttavia, la definizione e l'ambito di queste responsabilità rimangono ambigui, poiché i confini tra ciò che ricade sulle piattaforme e ciò che è responsabilità degli utenti sono spesso indefiniti.

3.6.1 Responsabilità delle piattaforme

Le piattaforme stabiliscono regole di comportamento che gli utenti devono rispettare per mantenere i propri account attivi e prevedono sanzioni per eventuali violazioni, che possono arrivare fino alla sospensione o al blocco permanente. Ad esempio, Meta ha adottato rigide politiche contro l'incitamento all'odio, i contenuti violenti e la disinformazione, specie nei contesti di salute pubblica e politica. TikTok, a sua volta, ha rafforzato le sue linee guida per contrastare il cyberbullismo e proteggere i suoi utenti più giovani. X, che storicamente ha favorito una maggiore libertà di espressione, è però sotto pressione per migliorare la gestione dei contenuti estremisti.

A livello giuridico, le piattaforme spesso si avvalgono delle disposizioni di "safe harbor", che limitano la loro responsabilità per i contenuti generati dagli utenti, a meno che non tollerino consapevolmente contenuti dannosi. Tuttavia, normative come il Digital Services Act nell'Unione Europea richiedono alle piattaforme di adottare misure proattive, introducendo nuove responsabilità per garantire la sicurezza degli utenti e il rispetto delle leggi.

3.6.2 Responsabilità degli utenti

Gli utenti, accettando i termini di utilizzo, si impegnano a rispettare le politiche comunitarie della piattaforma e a non pubblicare contenuti che violino le normative locali o le linee guida specifiche. Devono anche mantenere la sicurezza delle proprie credenziali di accesso e rispettare la privacy degli altri utenti. La pubblicazione di contenuti illeciti, come materiale protetto da copyright o discorsi d'odio, può comportare sanzioni legali. In questo senso, gli utenti hanno un ruolo attivo nella creazione di un ambiente online sicuro, poiché la loro partecipazione alle piattaforme comporta non solo diritti, ma anche obblighi verso la comunità.

In conclusione, la distinzione tra le responsabilità delle piattaforme e degli utenti evidenzia l'importanza di una collaborazione trasparente per garantire un ambiente digitale rispettoso e sicuro. Le piattaforme devono fornire strumenti chiari per la segnalazione e la moderazione dei contenuti, mentre agli utenti spetta il compito di utilizzarli in modo responsabile, contribuendo alla salute della community online.

3.7 Piattaforme a confronto

3.7.1 Panoramica dei termini di servizio

Meta (Facebook/Instagram)

I termini di servizio di Meta regolano l'accesso e l'utilizzo della piattaforma, specificando che l'azienda può raccogliere e utilizzare una vasta gamma di dati personali per la pubblicità e per ottimizzare l'esperienza utente. Gli utenti devono registrarsi con il loro nome reale e non possono usare pseudonimi, poiché la trasparenza è essenziale per la piattaforma. Meta permette la condivisione dei contenuti con specifici gruppi o individui, pur limitando alcune attività, come la creazione di account alternativi o la condivisione delle credenziali. L'azienda si riserva il diritto di sospendere gli account per diverse violazioni e di aggiornare i termini quando necessario[33].

X (Twitter)

La piattaforma consente l'uso di pseudonimi e permette agli utenti di esportare e archiviare i propri dati, rendendoli responsabili della sicurezza dell'account e delle attività su di esso. Tuttavia, X non garantisce continuità o assenza di errori del servizio, che può essere sospeso o limitato senza preavviso. Gli utenti sono informati dei rischi legati alla pubblicazione di informazioni personali online e possono scegliere con chi condividere i propri contenuti. Inoltre, il servizio monitora l'attività degli utenti, tracciando anche l'origine e le interazioni sul sito tramite cookie e altri strumenti di monitoraggio, ignorando le richieste "Do Not Track" (DNT)[34].

TikTok

TikTok consente agli utenti di mantenere la proprietà dei propri contenuti, ma può sospendere o cancellare account e contenuti senza preavviso per violazioni delle regole. Il servizio è fornito "così com'è" e non garantisce qualità o continuità, lasciando agli utenti la responsabilità di proteggere il proprio account. TikTok può aggiornare i termini e consiglia di verificarli regolarmente. L'uso dei cookie è obbligatorio per l'accesso a tutte le funzionalità, e il blocco può limitare l'esperienza d'uso[35].

3.7.2 Politiche sulla privacy e gestione dei dati

Meta (Facebook/Instagram)

Meta raccoglie una vasta gamma di dati personali, tra cui informazioni di localizzazione, cronologia di navigazione e dati biometrici[36][37][38][39], per scopi pubblicitari e personalizzazione dell'esperienza utente. Gli utenti possono scegliere con chi condividere i contenuti, ma devono accettare il tracciamento dei dati, che avviene anche tramite strumenti come cookie di terze parti, pixel di tracciamento e fingerprinting. Sebbene Meta dichiari di non vendere direttamente i dati personali, può condividerli con terze parti e trattenerli anche dopo la richiesta di cancellazione, se necessario per interessi aziendali o obblighi legali[33].

X (Twitter)

Il servizio raccoglie numerosi dati personali, incluse informazioni di localizzazione e attività su altri siti web, e utilizza queste informazioni per finalità pubblicitarie e di personalizzazione dei contenuti. X raccoglie dati tramite cookie di terze parti, tracking pixel e altre tecniche di tracciamento avanzate (ad es. browser fingerprinting), e memorizza informazioni anche per utenti che non interagiscono direttamente con la piattaforma. I dati possono essere condivisi con terze parti, venduti o trasferiti nel caso di operazioni finanziarie come una bancarotta. Inoltre, X conserva i contenuti eliminati dagli utenti e si riserva il diritto di utilizzare tali dati a propria discrezione, anche senza notifica preventiva[34].

TikTok

TikTok raccoglie una varietà di dati personali, inclusi dettagli di contatto, indirizzo IP, geolocalizzazione e dati biometrici, per pubblicità e personalizzazione del servizio. Tiktok ha anche la possibilità di leggere le conversazioni private tra utienti. Viene utilizzato anche il tracciamento tramite cookie e tecniche avanzate come i web beacon e il fingerprinting, e i dati possono essere condivisi con partner operativi e pubblicitari. TikTok mantiene la possibilità di trasferire o vendere questi dati globalmente per scopi aziendali e avvisa che il blocco dei cookie potrebbe limitare l'uso di alcune funzionalità[35].

3.7.3 Regole di comportamento e contenuti consentiti

Meta (Facebook/Instagram)

Gli utenti, sulla piattaforma, non è consentito promuovere o facilitare attività illegali e dalla distribuzione di materiale dannoso, inclusi contenuti su abusi su minori, autolesionismo, discriminazione, bullismo, e manipolazione psicologica o comportamentale. Non possono sfruttare persone vulnerabili o diffondere contenuti per adulti o ingannevoli come phishing o truffe. Anche i contenuti che minano la salute pubblica, come la promozione di droghe o armi, o che violano i diritti di altri, sono proibiti[33].

X (Twitter)

X non pone particolari limiti agli utenti, infatti specifica la possibili esposizioni a contenuti che potrebbero essere offensivi, dannosi, imprecisi o altrimenti inappropriati, o in alcuni casi, post che sono stati etichettati in modo errato o sono altrimenti ingannevoli e che la moderazione potrebbe essere assente. Tutti i Contenuti sono di esclusiva responsabilità della persona che li ha originati; potrebberp non controllare o monitorare i contenuti pubblicati tramite il servizio e che non possono essere responsabili di tali contenuti. x si riserva il diritto di rimuovere i contenuti che violano l'Accordo con l'Utente, tra cui, ad esempio, violazioni di copyright o di marchi o altre appropriazioni indebite di proprietà intellettuale, impersonificazione, condotta illecita o molestie[34].

TikTok

TikTok vieta agli utenti di creare account che impersonano altri individui. Sono vietati i contenuti volti a molestare, intimidire, o a promuovere violenza, discriminazione o contenuti sessualmente espliciti. Non si possono pubblicare contenuti coperti da copyright o contenenti dati privati di terzi. Sono vietati i contenuti contenenti pubblicità occulta. Qualsiasi contenuto volto che provoca, tormenta, spaventare o ferire qualcuno è vietato. Sono vietate minacce di qualsiasi tipo[35].

3.7.4 Diritti e responsabilità degli utenti

Meta (Facebook/Instagram)

Meta garantisce agli utenti il diritto di mantenere la proprietà dei propri contenuti e di lasciare la piattaforma in qualsiasi momento. Inoltre, offre opzioni per gestire la privacy e limitare la condivisione dei dati personali. Tuttavia, gli utenti devono usare il proprio nome legale, e Meta vieta l'uso di pseudonimi

per garantire trasparenza. Sono vietate attività illegali, comportamenti manipolativi, o la creazione di account multipli per evitare abusi e violazioni delle regole della piattaforma[33].

X (Twitter)

Gli utenti di X possono accedere, esportare e cancellare i propri dati e scegliere con chi condividere i contenuti. È possibile utilizzare pseudonimi, ma gli utenti sono responsabili della sicurezza del proprio account e delle attività svolte tramite esso. X consente libertà di pubblicazione, ma proibisce messaggi indesiderati e tentativi di accesso non autorizzato. X può rimuovere contenuti o chiudere account senza preavviso per violazioni o a propria discrezione. Gli utenti devono rispettare le leggi applicabili e sono informati che i propri dati potrebbero essere conservati, trasferiti o divulgati a terzi in specifiche circostanze, come procedimenti legali o bancarotta[34].

TikTok

Gli utenti di TikTok mantengono la proprietà dei propri dati e sono responsabili per il rispetto dei Termini di Servizio, incluso non violare diritti di copyright o norme della piattaforma. In caso di violazioni, TikTok può sospendere o eliminare l'account e i contenuti dell'utente senza preavviso. Gli utenti accettano inoltre di rinunciare ai diritti di azioni collettive e di sottostare a clausole di arbitrato per eventuali dispute. TikTok si riserva il diritto di modificare i contenuti pubblicati dagli utenti per qualsiasi motivo e non garantisce l'accuratezza delle informazioni o la continuità del servizio[35].

3.7.5 Differenze

Tra le piattaforme Meta (Facebook/Instagram), X (Twitter) e TikTok, emergono differenze significative nelle regole di comportamento, la gestione dei dati e la moderazione dei contenuti. Meta, ad esempio, richiede agli utenti di registrarsi con il proprio nome reale per garantire la trasparenza e limita la creazione di account multipli, mentre X permette pseudonimi e accetta la possibilità di account multipli. Inoltre, mentre Meta e TikTok applicano normative rigide per moderare contenuti dannosi o violenti e vietano espressamente contenuti che incitano alla violenza, X lascia maggiore libertà di pubblicazione e avverte gli utenti della possibilità di imbattersi in contenuti offensivi o inaccurati, riservandosi comunque il diritto di rimuovere contenuti che violano i termini di servizio. Anche in ambito di trattamento dei dati, TikTok raccoglie e utilizza dati biometrici e altre informazioni personali per

personalizzare i servizi, un aspetto che si distingue dalle altre piattaforme che tendono a dare più opzioni di controllo sui dati.

3.7.6 Aspetti Comuni

Un aspetto comune a tutte e tre le piattaforme è la politica di tutela dei diritti di proprietà degli utenti sui propri contenuti, sebbene con alcune limitazioni. Meta, X e TikTok, infatti, consentono agli utenti di mantenere la proprietà del materiale che pubblicano, ma ciascuna piattaforma può intervenire e rimuovere contenuti in caso di violazione dei rispettivi termini di servizio. Le tre piattaforme applicano inoltre un sistema di tracciamento degli utenti per finalità pubblicitarie, che include strumenti avanzati come cookie e pixel di tracciamento, e informano gli utenti dell'eventuale condivisione dei dati con terze parti, soprattutto per finalità pubblicitarie o di ottimizzazione del servizio.

3.8 In Conclusione

Le attuali pratiche di regolamentazione dei social media, che prevedono politiche di moderazione autonome per ciascuna piattaforma, presentano sfide complesse sia per gli utenti sia per le piattaforme stesse. Gli utenti, infatti, devono navigare tra termini di servizio che variano molto e che possono essere modificati unilateralmente, con impatti su privacy e libertà di espressione. La crescente raccolta e utilizzo di dati personali, spesso condivisi con terze parti per fini commerciali, solleva preoccupazioni etiche e giuridiche sulla tutela della privacy e sulla sicurezza dei dati. Dal lato delle piattaforme, queste devono affrontare la difficoltà di bilanciare la moderazione dei contenuti e la libertà di espressione, gestendo responsabilità legali, aspettative degli utenti e possibili interventi normativi. La sfida si complica ulteriormente considerando l'incremento di fake news, hate speech e altri contenuti dannosi, richiedendo un equilibrio tra la rimozione di tali contenuti e tutelare la libertà di parola.

Le prospettive future di regolamentazione si muovono verso normative più uniformi e internazionali, che impongano requisiti di trasparenza e accountability delle piattaforme, come si sta osservando con il *Digital Services Act*[40] dell'Unione Europea. Questo atto legislativo mira a creare un ambiente digitale più sicuro e responsabile, imponendo alle piattaforme di dimostrare come gestiscono i contenuti e proteggono i dati degli utenti. In futuro, regolamenti più chiari e standardizzati potrebbero aiutare a uniformare le regole e a ridurre l'ambiguità, imponendo alle piattaforme limiti più stringenti nella raccolta di dati e trasparenza sui processi di moderazione. Tuttavia, una regolamentazione

troppo rigida potrebbe anche ridurre la libertà delle piattaforme di adattare i propri servizi alle esigenze di specifici mercati, portando a una maggiore tensione tra innovazione e conformità normativa. Questo equilibrio delicato richiederà un dialogo continuo tra governi, piattaforme digitali e utenti per garantire che le normative evolvano in modo efficace e rispettoso dei diritti di tutte le parti coinvolte.

Capitolo 4

Idee e Prospettive

4.1 I Social come luoghi aperti al pubblico moderni: la Necessità di Identificazione

A conclusione di questo lavoro di tesi, una riflessione generale è rivolta ai social media che possono essere visti come bar, piazze o circoli associativi "digitalizzati", luoghi pubblici dove individui e gruppi si incontrano per socializzare, scambiarsi idee e raccontarsi, una opportunità sociale e individuale. In questi contesti, è consuetudine presentarsi con un'identità riconoscibile, anche per rispettare le norme di convivenza sociale; inoltre l'articolo 5 delle *Disposizioni a tutela dell'ordine pubblico* dispone che non si possa fare uso di mezzi che rendano difficoltosi il riconoscimento della persona[41]. Proprio come nessuno si aggirerebbe in un bar senza un documento di riconoscimento o, in termini più moderni, una forma di "accountability" sociale, anche i social media, in quanto "spazi pubblici" digitali, potrebbero beneficiare di un sistema di verifica dell'identità che promuova comportamenti più rispettosi.

La scelta di considerare i social media e Internet come luoghi pubblici riflette un'evoluzione nella nostra concezione di spazi comuni, resa necessaria dalla crescente digitalizzazione. La vita moderna, sempre più intrecciata al mondo online, ha portato a una transizione: dalle interazioni fisiche, limitate a contesti specifici come il quartiere o la città, a interazioni virtuali che ampliano la nostra rete sociale su scala globale. In questa nuova dimensione pubblica, le piattaforme digitali diventano spazi aperti in cui la società si ritrova, si esprime e si identifica, proprio come nei luoghi di ritrovo tradizionali. Tuttavia, la natura apparentemente "anonima" di questi spazi virtuali solleva nuove sfide per la gestione di comportamenti e responsabilità individuali.

Riconoscere l'online come un luogo aperto al pubblico implica stabilire nuovi standard di comportamento e una maggiore accountability, per proteggere l'esperienza degli utenti e mantenere la sicurezza del contesto virtuale. Questa concezione suggerisce una regolamentazione che preservi i diritti di espressione e garantisca il rispetto delle norme di convivenza civile, proprio come avviene in qualsiasi altro ambiente pubblico.

4.2 Un Sistema di Verifica dell'Identità per la Responsabilità Online

Un sistema di verifica dell'identità che bilanci privacy e responsabilità potrebbe basarsi su un meccanismo di token anonimo generato dallo Stato. Durante la registrazione a un servizio online, verrebbe richiesto all'utente di autenticarsi con una forma di identificazione elettronica riconosciuta, come la Carta d'Identità Elettronica (CIE). Questo primo passaggio conferma l'identità reale dell'utente senza che vengano trasmessi dettagli personali al servizio.

A seguito dell'autenticazione, il sistema dello Stato genera un token unico che è associato solo all'identità verificata dell'utente e non al servizio specifico. Questo token è memorizzato in un database pubblico, ma resta privo di informazioni sul servizio al quale l'utente intende registrarsi. In questo modo, l'identità legale è conservata e separata dall'identità online dell'utente, salvaguardando la privacy.

Il servizio riceve il token e lo lega all'account dell'utente senza ricevere ulteriori dati personali, come nome, età o genere, lasciando così libertà all'utente di esprimersi liberamente e autonomamente online registrandosi con i dati che preferisce. Questo offre un certo grado di anonimato, mantenendo la privacy senza compromettere la validità della registrazione. Tuttavia, in caso di necessità lo Stato, solo attraverso con un mandato disposto dall'autorità giudiziaria, potrebbe richiedere al servizio il token legato all'account. In questo caso, il token consente di risalire all'identità reale dell'utente, ma soltanto per finalità che giustifichino una violazione della privacy.

Questo approccio bilancia la tutela dell'anonimato online con la responsabilità sociale, limitando l'identificazione alle sole circostanze eccezionali e giuridicamente fondate. Ne deriverebbe un ambiente online più sicuro, in cui gli utenti sono incentivati a comportarsi in modo più responsabile, sapendo che, in situazioni gravi e comprovate, la loro identità può essere rivelata secondo legge.

4.2.1 Punti di forza

Sicurezza dell'Identità

Il sistema garantisce un elevato livello di sicurezza per quanto riguarda la tutela dell'identità dell'utente. Solo le autorità giudiziarie, in possesso di un mandato, possono risalire all'identità reale dell'utente tramite il token. Questo assicura che le piattaforme non abbiano accesso diretto ai dati personali dell'utente, riducendo i rischi di compromissione della privacy a livello di servizio.

Protezione della Privacy degli Utenti

La gestione separata tra Stato e piattaforme garantisce che i dati personali non vengano memorizzati da terzi. Il token è anonimo per il servizio e viene generato senza includere informazioni identificative, consentendo agli utenti di mantenere un livello di riservatezza pur rispettando i requisiti legali.

Riduzione dell'Anonimato Danno-Produttivo

Il sistema limita l'anonimato solo in casi specifici e previa autorizzazione di un tribunale, scoraggiando comportamenti antisociali e illeciti. La consapevolezza che le autorità possono risalire all'identità reale dell'utente in caso di abusi contribuisce a un ambiente online più sicuro e responsabile.

4.2.2 Debolezze

Costi e Complessità Implementativa

L'adozione del sistema richiederebbe infrastrutture idonee a memorizzare in sicurezza tutti i token comporterebbe costi considerevoli per lo Stato. Perdere o disperdere questi dati sarebbe deleterio, o per la consistenza del sitema o per la privacy degli utenti.

Doppia Autenticazione Necessaria

Poiché il token non può essere usato per l'autenticazione, gli utenti dovranno comunque creare e ricordare username e password. Questo potrebbe generare una percezione di complessità nei processi di registrazione, riducendo l'adesione spontanea al sistema riducendone l'efficacia.

Possibili Resistenze per Questioni di Privacy e Libertà

Alcuni utenti potrebbero percepire il sistema come un'invasione della loro privacy, temendo un controllo governativo troppo pervasivo. Questo potrebbe incontrare resistenze, soprattutto da parte di gruppi sensibili alla privacy e alla libertà di espressione.

4.2.3 Opportunità

Supporto all'Integrità delle Piattaforme Social

L'introduzione di questo sistema di verifica potrebbe aumentare la fiducia e la sicurezza nelle piattaforme social, incentivando una partecipazione più rispettosa e trasparente. Con un ambiente digitale più controllato, si potrebbero attrarre utenti che altrimenti eviterebbero le piattaforme per paura di attacchi o di molestie anonime.

Applicazioni Internazionali

Un sistema del genere potrebbe essere adottato in modo uniforme in diversi paesi, portando a una regolamentazione internazionale dell'identità digitale. Questo potrebbe contribuire a ridurre fenomeni come la criminalità transfrontaliera, le truffe e l'hate speech su scala globale.

Sostegno per la Prevenzione del Crimine

Consentendo l'accesso ai dati identificativi solo in casi giustificati, le autorità potrebbero intervenire tempestivamente in caso di attività criminali, salvaguardando gli utenti e prevenendo il crimine, ma senza interferire con la normale esperienza di navigazione.

4.2.4 Rischi

Rischi di Abuso da Parte delle Autorità

Sebbene il sistema preveda l'accesso ai dati solo con un mandato, c'è il rischio di un abuso di potere o di interpretazioni estensive della legge, che potrebbero compromettere la fiducia nel sistema. La possibilità di ottenere i dati potrebbe essere soggetta a pressioni politiche, portando a controversie.

Perdita di Utenti che Preferiscono l'Anonimato

Alcuni utenti potrebbero abbandonare le piattaforme che richiedono questo tipo di verifica per paura di perdere l'anonimato. Questo rischio è particolar-

mente elevato tra i gruppi che difendono il diritto alla privacy e tra gli utenti di piattaforme specializzate in discussioni politiche o di attualità sensibili.

Sfide Tecnologiche e Cybersecurity

Un sistema che memorizza token legati all'identità digitale degli utenti potrebbe diventare bersaglio di attacchi informatici. Eventuali compromissioni potrebbero esporre milioni di identità e causare danni considerevoli sia agli utenti che alle istituzioni coinvolte.

Bibliografia

[1] GfK Sinottica®. Gfk sinottica®: italiani preoccupati e poco informati sulla privacy. https://www.gfk.com/it/stampa/gfk-sinottica-italiani-preoccupati-e-ancora-poco-informati-sulla-privacy-online.

[2] Google. How chrome incognito keeps your browsing private. https://support.google.com/chrome/answer/9845881?hl=en#zippy=%2Chow-incognito-mode-works%2Chow-incognito-mode-protects-your-privacy%2Cyoure-in-control.

[3] Polizia Postale. Pillole di sicurezza informatica o igiene informatica (cyber hygiene). cos'è? https://www.commissariatodips.it/approfondimenti/cyber-hygiene/pillole-di-sicurezza-informatica-o-igiene-informatica-cyber-hygiene-cose/index.html.

[4] Sunwoo Adela Cho. The power of virtual private networks (vpn) in privacy protection. https://informationsecurity.wustl.edu/the-power-of-virtual-private-networks-vpn-in-privacy-protection/, 2024.

[5] English Wikipedia user HANtwister. Svg diagram of the "onion routing" principle. https://it.wikipedia.org/wiki/Onion_routing#/media/File:Onion_diagram.svg, 2008.

[6] Bruce Schneier. Attacking tor: how the nsa targets users' online anonymity. *The Guardian*. https://cyber-peace.org/wp-content/uploads/2013/06/Attacking-Tor_-how-the-NSA-targets-users-online-anonymity-_-World-news-_-theguardian.pdf.

[7] I. Karunanayake, N. Ahmed, R. Malaney, M. R. Islam, and S. Jha. De-anonymisation attacks on tor: A survey. *IEEE Communications Surveys & Tutorials*, PP:1–1, 07 2021. https://www.researchgate.net/figure/Attack-Scenario-with-compromised-Entry-and-Exit-nodes_fig5_352938766.

[8] PyNetLabs. What is mac address and how to find it? https://www.pynetlabs.com/what-is-mac-address/, 2024.

[9] Metin UZAR. Basic informations about gsm networks. https://razunitem.wordpress.com/2009/11/06/basic-informations-about-gsm-networks/, 2009.

[10] E. Roosevelt, P.C. Chang, C. Malik, W.R. Hodgson, H. Hernán Santa Cruz, R. Cassin, A.E. Bogomolov, C. Dukes, and J.P. Himphrey. Universal declaration of human rights. *United Nations*. https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/itn.pdf.

[11] Unated Nations General Assembly. The right to privacy in the digital age. *United Nations*. https://documents.un.org/doc/undoc/gen/n13/449/47/pdf/n1344947.pdf.

[12] Unated Nations General Assembly. The promotion, protection and enjoyment of human rights on the internet. *United Nations*. https://documents.un.org/doc/undoc/gen/g16/156/90/pdf/g1615690.pdf.

[13] S. Medvedev and I. Goryachev. Yarovaya law and new data storage requirements for online data distributors. *International Law Office*. https://www.gorodissky.com/upload/articles/files/Yarovaya_Law_and_new_data_storage_requirements.pdf.

[14] European Union. Article 8 - protection of personal data. *Charter of Fundamental Rights of the European Union*. https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data.

[15] European Union. Article 11 - freedom of expression and information. *Charter of Fundamental Rights of the European Union*. https://fra.europa.eu/en/eu-charter/article/11-freedom-expression-and-information.

[16] European Union. General data protection regulation. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[17] European Union. Directive on privacy and electronic communications. *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058.

[18] European Court Of Human Rights. Case of k.u. v. finland. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-89964%22]}.

[19] Assemblea Costituente. Articolo 21. *Costituzione della Repubblica Italiana*. https://www.senato.it/istituzione/la-costituzione/parte-i/titolo-i/articolo-21.

[20] Garante per la Protezione dei Dati Personali. Decreto legislativo 30 giugno 2003, n.196 recante il "codice in materia di protezione dei dati personal". https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29.

[21] Grand Chamber of the European Court of Human Rights. Google spain sl and google inc. v agencia española de protección de datos (aepd) and mario costeja gonzález. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

[22] OECD. How's life in the digital age? https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/02/how-s-life-in-the-digital-age_g1g9e413/9789264311800-en.pdf, 2019.

[23] Caroline Cakebread. You're not alone, no one reads terms of service agreements. https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11, 2017.

[24] Statista. Distribution of facebook users worldwide as of april 2024, by age and gender. https://www.statista.com/statistics/376128/facebook-global-user-age-distribution/, 2024.

[25] Statista. Distribution of instagram users worldwide as of april 2024, by age and gender. https://www.statista.com/statistics/248769/age-distribution-of-worldwide-instagram-users/, 2024.

[26] Statista. Leading countries based on number of x (formerly twitter) users as of april 2024. https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/, 2024.

[27] Statista. Distribution of x (formerly twitter) users worldwide as of january 2024, by age group and gender. https://www.statista.com/statistics/1498204/distribution-of-users-on-twitter-worldwide-age-and-gender/, 2024.

[28] Statista. Distribution of tiktok users worldwide as of july 2024, by age and gender. https://www.statista.com/statistics/1299771/tiktok-global-user-age-distribution/, 2024.

[29] The New York Times. A third of tiktok's u.s. users may be 14 or under, raising safety questions. https://www.nytimes.com/2020/08/14/technology/tiktok-underage-users-ftc.html, 2020.

[30] Statista. Countries with the largest tiktok audience as of july 2024. https://www.statista.com/statistics/1299807/number-of-monthly-unique-tiktok-users/#:~:text=As%20of%20July%202024%2C%20Indonesia,on%20TikTok%20watching%20short%2Dvideos., 2024.

[31] Natasha Lomas. Meta fined $101.5m for 2019 breach that exposed hundreds of millions of facebook passwords. https://techcrunch.com/2024/09/27/meta-fined-101-5m-for-2019-breach-that-exposed-hundreds-of-millions-of-facebook-passwords/, 2024.

[32] Repubblica Italiana. Esercizio di un diritto o adempimento di un dovere. https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.progressivo=0&art.idArticolo=51&art.versione=1&art.codiceRedazionale=030U1398&art.dataPubblicazioneGazzetta=1930-10-26&art.idGruppo=5&art.idSottoArticolo1=10&art.idSottoArticolo=1&art.flagTipoArticolo=1#:~:text=51)-,Art.,'%2C%20esclude%20la%20punibilita'.

[33] ToS;DR. Facebook terms of service. https://edit.tosdr.org/services/182/annotate#doc_22996.

[34] ToS;DR. X terms of service. https://edit.tosdr.org/services/195/annotate/.

[35] ToS;DR. Tiktok terms of service. https://edit.tosdr.org/services/1448/annotate/#doc_1084.

[36] ToS;DR. The service collects many different types of personal data. https://edit.tosdr.org/points/10688.

[37] ToS;DR. This service may collect, use, and share location data. https://edit.tosdr.org/points/10686.

[38] ToS;DR. This service can view your browser history. https://edit.tosdr.org/points/17261.

[39] ToS;DR. Your biometric data is collected. https://edit.tosdr.org/points/12118.

[40] Unione Europea. Digital services act. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2065, 2022.

[41] Repubblica Italiana. Legge 8 agosto 1922, n.533 art.2. https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.versione=1&art.idGruppo=0&art.flagTipoArticolo=0&art.codiceRedazionale=077U0533&art.idArticolo=2&art.idSottoArticolo=1&art.idSottoArticolo1=10&art.dataPubblicazioneGazzetta=1977-08-20&art.progressivo=0#art, 1977.

Elenco delle figure