Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Il Consiglio federale

15 dicembre 2022

Discorsi di odio. Ci sono lacune nella legislazione?

Rapporto del Consiglio federale in adempimento del postulato 21.3450 della Commissione della politica di sicurezza del Consiglio degli Stati del 25 marzo 2021

Bericht Postulat SiK 21.3450 "Hassreden. Bestehen gesetzliche Lücken?"_18.11.2022

Sintesi

Il postulato 21.3450 della Commissione della politica di sicurezza del Consiglio degli Stati (CPS-S) del 25 marzo 2021 recita:

> **Testo:** Il Consiglio federale è incaricato di presentare un rapporto che tracci un quadro delle misure e dei mezzi di diritto penale, di polizia preventiva e di diritto pubblico (per es. diritto delle telecomunicazioni) che esistono per lottare contro le incitazioni pubbliche all'odio (discorsi di odio) e contro l'importazione e la diffusione di materiale di propaganda estremista. Il rapporto dovrà inoltre indicare le eventuali lacune a livello legislativo.

I discorsi di odio costituiscono una minaccia per la coesione e la sicurezza pubblica delle società democratiche, in quanto denigrano persone e gruppi sociali, negando loro una partecipazione equa alla vita sociale e impedendo loro di esprimersi liberamente. Diffondono altresì ideologie estremiste (violente) e possono portare alla radicalizzazione degli individui. Le vittime dei discorsi di odio invece tendono a ritirarsi dalla sfera pubblica. Il presente rapporto traccia un quadro delle misure di diritto penale e pubblico, in particolare di polizia preventiva, che esistono per lottare contro l'incitamento all'odio, e indica le principali sfide. Illustra, seppur in misura minore, anche la situazione del diritto civile.

Nel rapporto si fa riferimento alla definizione di discorso di odio del Consiglio d'Europa, che lo intende come la denigrazione di individui o gruppi di persone in base a determinate caratteristiche (sociali) e come la diffusione di materiale diffamatorio. Sebbene l'incitamento all'odio si manifesti sia offline che online, la sua divulgazione avviene sempre più tramite le piattaforme degli intermediari digitali come Facebook, YouTube o TikTok, che negli ultimi anni sono diventati i canali principali per la comunicazione pubblica. Il rapporto si concentra quindi anche sulla sfera digitale, soprattutto perché è in quest'ambito che si presentano le principali sfide sul piano giuridico.

Le piattaforme dei social media offrono ai loro utenti un facile accesso alla sfera pubblica, garantiscono l'anonimato, puntano sui contenuti aperti e incrementano la portata dell'*user-generated content*. Questi elementi promuovono la visibilità e la propagazione dei contenuti, possono ampliare il discorso democratico ma anche portare alla divulgazione di massa e spesso mirata dell'odio.

L'odio online può trasformarsi in violenza nel mondo reale o favorire gli atti violenti. Gli episodi offline, ossia nel mondo reale, possono invece alimentare l'odio online, creando un processo di auto rafforzamento. Il controllo svolto sulle piattaforme da persone e algoritmi risulta contradditorio e inefficiente. Inoltre, gli standard di espressione consentiti variano assai notevolmente da una piattaforma all'altra e gli approcci più rigorosi fanno spostare l'odio su piattaforme con poche limitazioni a livello di contenuti.

Sul piano politico, di recente questa minaccia per la società è stata affrontata più volte in Svizzera. Diversi interventi parlamentari trattano la portata dei discorsi di odio sulle piattaforme digitali e auspicano una maggiore trasparenza da parte dei gestori. Nella maggior parte dei casi ci si interroga su come contrastare quest'odio e fare in modo che gli intermediari si assumano più responsabilità.

L'UE e altri Paesi europei contrastano la diffusione dell'odio online all'interno di un proprio quadro normativo che crea maggiori responsabilità per gli intermediari attraverso obblighi di diligenza specifici. Oltre alle basi legali di singoli Stati come la *Netzwerkdurchsetzungsgesetz* in Germania o la *Online Safety Bill* del Regno Unito, la legge sui servizi digitali (Digital Services Act) dell'Unione europea, entrata in vigore a fine 2022, costituisce l'approccio più completo in questo ambito. Secondo tale legge, in particolare le piattaforme online di grandi dimensioni devono sottostare a una serie di norme in materia di obblighi di diligenza.

In Svizzera il diritto penale è il mezzo migliore per contrastare i discorsi di odio e la loro diffusione. Tuttavia, sebbene si possano applicare diverse disposizioni, ovvero la rappresentazione di atti di cruda violenza (art. 135 CP), i delitti contro l'onore (art. 173 segg. CP), le minacce (art. 180 CP), la coazione (art. 181 CP) nonché i crimini o i delitti contro la tranquillità pubblica (art. 258 segg. CP), in particolare la pubblica istigazione a un crimine o alla violenza (art. 259 CP), nonché la discriminazione e l'incitamento all'odio (art. 261bis CP), il concetto non compare espressamente nel diritto svizzero attualmente in vigore.

Bericht Postulat SiK 21.3450 "Hassreden. Bestehen gesetzliche Lücken?"_18.11.2022

Dal punto di vista del diritto penale non si fa distinzione tra i discorsi di odio online e offline, se non che i primi avvengono con l'ausilio di tecnologie digitali confacenti allo scopo. La sfida principale è infatti correlata al fatto che generalmente, i dati si trovano su server esteri, il che conferisce alla questione dell'applicazione del diritto un carattere internazionale e riduce notevolmente le prospettive di successo del procedimento penale. Di conseguenza, soprattutto la soppressione di contenuti illegali è spesso possibile soltanto se gli intermediari sono disposti a collaborare di propria iniziativa.

Un quadro simile emerge nel settore del diritto civile. Anche in questo caso si pongono gli stessi problemi di applicazione del diritto, come in ambito penale. In entrambi i casi contrastare i discorsi di odio non è reso difficile dalla mancanza di disposizioni materiali ma piuttosto da lacune in relazione all'applicazione del diritto vigente.

Oltre a questi ambiti giuridici, si aggiungono ulteriori disposizioni di diritto pubblico. Si tratta di misure preventive di polizia riguardanti la diffusione di materiale di propaganda, la protezione di autorità ed edifici e il mondo online. La legge sulla radiotelevisione, la legge sulla protezione dei minori nei settori dei film e dei videogiochi così come la legge sulla protezione dei dati e la legge sulle telecomunicazioni comprendono disposizioni che trattano il fenomeno della diffamazione di individui e gruppi di persone sulla base di determinate caratteristiche sociali. Nella maggior parte dei casi, tuttavia, la rilevanza pratica è piuttosto bassa.

Con il Digital Services Act, l'UE persegue un approccio che impone alle piattaforme una serie di obblighi nei confronti dei loro utenti. In Svizzera l'UFCOM, in collaborazione con la Cancelleria federale, ha pubblicato nel 2021 il rapporto "Intermediari e piattaforme di comunicazione. Effetti sulla comunicazione pubblica e approcci di governance", che esamina il potenziale positivo e negativo a livello sociale delle piattaforme digitali, e illustra gli approcci in materia di regolamentazione presenti in Europa. Successivamente, l'UFCOM ha elaborato un documento di discussione all'attenzione del Consiglio federale, il quale indica se e come gli intermediari digitali necessitano di una regolamentazione. Il 5 aprile 2023, il Consiglio federale ha incaricato il DATEC (UFCOM) di preparare un progetto di consultazione sulla regolamentazione delle piattaforme di comunicazione.

Sulla base del rapporto sulla responsabilità civile dei provider, il Consiglio federale ha inoltre dato priorità alla conclusione di accordi di assistenza legale reciproca e di convenzioni che prevedono il recapito postale diretto di documenti in materia civile.

Nell'ambito delle misure preventive di polizia, nel 2019 il Consiglio nazionale e il Consiglio degli Stati hanno accolto la mozione "Scambio di dati di polizia su scala nazionale" (Mo. 18.3592), in base alla quale le autorità di polizia cantonali devono avere la possibilità di scambiarsi sistematicamente informazioni di polizia tra di loro e con gli organi di polizia della Confederazione. L'attuazione è ora affidata al Consiglio federale.

Sono inoltre necessari miglioramenti anche nella gestione delle minacce affinché l'odio e l'incitamento all'odio possano essere riconosciuti e combattuti meglio. Le lacune riguardano soprattutto lo scambio di informazioni tra Confederazione e Cantoni, i diritti di accesso e l'analisi automatizzata dei dati.

Infine il 30 settembre 2022 il Consiglio nazionale e il Consiglio degli Stati hanno adottato la legge federale sulla protezione dei minori nei settori dei film e dei videogiochi (LPMFV; FF *2022* 2406). Questa prevede l'obbligo di istituire sistemi di segnalazione che possano contribuire a frenare la diffusione e la visibilità dei discorsi di odio.

Il Consiglio federale non vede quindi al momento alcuna necessità di adottare misure supplementari oltre a quelle summenzionate.

Bericht Postulat SiK 21.3450 "Hassreden. Bestehen gesetzliche Lücken?"_18.11.2022

Indice

Bericht Postulat SiK 21.3450 "Hassreden. Bestehen gesetzliche Lücken?"_18.11.2022

1 Situazione iniziale e mandato

Negli ultimi anni i discorsi di odio sono aumentati in particolare nell'area commenti dei siti web di notizie nonché sulle piattaforme degli intermediari digitali e sono ora percepiti come un serio problema sociale. La diffusione di tali discorsi sulle reti digitali transnazionali pone le autorità di fronte a nuove sfide relative all'esecuzione del diritto vigente.

1.1 Postulato

Alla luce di quanto esposto, con il postulato 21.3450 la Commissione della politica di sicurezza del Consiglio degli Stati (CPS-S) ha incaricato il Consiglio federale di tracciare un quadro delle misure legali esistenti e di rilevare le possibili sfide.

In concreto il postulato incarica il Consiglio federale di "presentare un rapporto che tracci un quadro delle misure e dei mezzi di diritto penale, di polizia preventiva e di diritto pubblico (per es. diritto delle telecomunicazioni) che esistono per lottare contro le incitazioni pubbliche all'odio (discorsi di odio) e contro l'importazione e la diffusione di materiale di propaganda estremista. Il rapporto dovrà inoltre indicare le eventuali lacune a livello legislativo".

Il presente rapporto, di competenza dell'Ufficio federale delle comunicazioni (UFCOM), è stato redatto insieme all'Ufficio federale di giustizia (UFG) e in collaborazione con fedpol.

1.2 Struttura del rapporto

Il rapporto è suddiviso in cinque parti. Il prossimo capitolo (cap. 2) illustra il fenomeno dell'incitamento all'odio dal punto di vista delle scienze sociali e descrive gli interventi politici attuali sulla tematica. Il capitolo 3 colloca l'incitamento all'odio nel contesto internazionale, in particolare attraverso i progetti di legge dell'UE e di singoli Stati europei nel settore digitale. Il capitolo successivo costituisce il nucleo di questo rapporto ed esamina le misure di diritto penale (cap. 4.2), di polizia preventiva (cap. 4.4.1) e altre possibilità offerte dal diritto pubblico (cap. 4.4.2) nella lotta contro i discorsi di odio e illustra le sfide legislative in tale ambito; il capitolo è concluso da un excursus sugli strumenti di diritto privato. La conclusione (cap. 5) riassume i risultati e identifica gli ambiti in cui occorre agire con maggiore urgenza.

Il rapporto esclude volutamente dalla sua analisi due settori, che fanno parte di un discorso più approfondito sul tema dell'incitamento all'odio. In primo luogo, si limita a esaminare il ruolo degli intermediari digitali nella diffusione dei discorsi di odio e la questione dell'applicazione della legge alle piattaforme pubbliche, ossia ai social network come Facebook, YouTube o TikTok. I servizi (semi)privati come WhatsApp non rientrano invece nell'analisi. In secondo luogo, il presente rapporto si concentra sul discorso di odio secondo la definizione del Consiglio d'Europa ed esclude in larga misura fenomeni correlati come l'estremismo violento e il terrorismo.

1.3 Termini principali: discorso di odio e piattaforme digitali

Il concetto di **discorso di odio** non rappresenta una categoria ben definita né dal profilo (socio)scientifico né da quello giuridico. Si tratta piuttosto, in particolare nella tradizione giuridica europea, di una denominazione collettiva relativamente nuova, che comprende diverse forme di discriminazione, denigrazione o minacce di violenza. La definizione più concreta, utilizzata anche nel rapporto, deriva dalla raccomandazione del Comitato dei Ministri del Consiglio d'Europa agli Stati membri per la lotta contro i discorsi di odio, ovvero:

> qualsiasi forma di espressione che inciti, promuova, diffonda o giustifichi violenza, odio o discriminazione contro una persona o un gruppo di individui, o lo denigri per le caratteristiche personali reali o attribuite o lo status, come ad esempio per motivi di "razza", colore della pelle, lingua, religione, nazionalità, origine nazionale o etnica, età, disabilità, genere, identità di genere e orientamento sessuale[1].

Inoltre, il Consiglio d'Europa propone una gradazione delle misure (legali) contro i discorsi di odio in base al loro grado di gravità, al danno che provocano e alle conseguenze per i membri di

[1] COUNCIL OF EUROPE (2022), Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech.

determinati gruppi sociali. Il Consiglio d'Europa suddivide quindi i discorsi di odio in due categorie. La prima comprende le forme di incitamento all'odio che sono (a) vietate dal diritto penale e (b) che possono essere punite in base al diritto civile o amministrativo. Da questa vanno distinte le affermazioni denigratorie che non dovrebbero primariamente essere contrastate tramite le vie legali ma che comunque richiedono misure come ad esempio vari programmi nel campo dell'istruzione o del dialogo interculturale, nonché misure di sensibilizzazione[2].

Il presente rapporto si limita alle possibilità legali e alle sfide per contrastare i discorsi e la propaganda di odio, trascurando altre misure non di stampo legale.

Le piattaforme digitali, i "social media" o "media sociali" sono intesi come termine generale per indicare le piattaforme dei media sociali e quelle multimediali, nonché i servizi di microblogging come Facebook, YouTube o TikTok, che consentono sia gli scambi reciproci fra contatti già stabiliti ("amici", "follower", ecc.), sia la pubblicazione di contenuti rivolti a un pubblico potenzialmente illimitato. Sulla maggior parte delle piattaforme è inoltre possibile reagire ai contenuti pubblicati ("like", "retweet", ecc.). La comunicazione sulle piattaforme può anche avvenire con l'ausilio di programmi informatici (cosidd. "bot"[3]). A seconda del servizio, i contenuti pubblicati possono essere elaborati, diffusi e fruiti principalmente in forma di testo (ad. es. sul servizio di microblogging X, ex Twitter), immagini (ad es. su Instagram) o video (ad es. YouTube). Di norma è possibile anche mescolare le tipologie di contenuto (ad es. una foto con un relativo commento in forma testuale). Questa definizione non comprende i servizi propriamente di messaggistica come WhatsApp, la cui comunicazione è prevalentemente di carattere privato, sebbene la transizione tra la comunicazione privata e quella pubblica sia sempre più dinamica in ambito digitale sulle piattaforme e i servizi di messaggistica.[4]

[2] COUNCIL OF EUROPE (2022), Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech.

[3] I bot sono programmi informatici che svolgono compiti ripetitivi in modo sempre più automatizzato. Nel campo della comunicazione, ad esempio, sono programmati per partecipare a discussioni e per rispondere automaticamente a determinati commenti.

[4] Infatti, le comunicazioni private, ad esempio nei gruppi di messaggeria, possono aprire la strada a (ulteriori) discorsi pubblici di odio o incitare alla violenza.

2 L'incitamento all'odio come problema sociale e sfida politica

I discorsi di odio minacciano l'integrità dei sistemi democratici in diversi modi. Innanzitutto, denigrano persone e interi gruppi sociali, violano la loro dignità e li escludono da una partecipazione equa alla vita sociale. I discorsi di odio negano alle persone colpite i loro diritti umani fondamentali e impediscono loro di esprimersi liberamente; di conseguenza, le vittime di tali discorsi tendono a ritirarsi dalla sfera pubblica. I discorsi di odio, soprattutto online, possono anche contribuire alla radicalizzazione delle persone. La diffusione e la tolleranza dei discorsi di odio possono rendere l'odio e le relative ideologie (violente) qualcosa di normale. Tali discorsi possono quindi preparare il terreno per la violenza fisica e le atrocità, compreso il genocidio.

L'incitamento all'odio non è un fenomeno nuovo ma esiste già da molto prima della digitalizzazione. L'avvento di Internet e, in particolare, la creazione di piattaforme globali nella sfera pubblica digitale come YouTube, Instagram o TikTok ha acuito ulteriormente il problema e gli ha conferito una nuova dimensione. È proprio il fatto che si tratti di piattaforme di comunicazione aperte che promuove i potenziali positivi e negativi e porta a una propagazione praticamente indisturbata dei discorsi di odio. Quattro fattori giocano un ruolo particolarmente decisivo, come spiegato in dettaglio anche nel rapporto dell'UFCOM "Intermediari e piattaforme di comunicazione"[5].

Primo: le piattaforme digitali e i motori di ricerca semplificano la reperibilità delle informazioni e la loro diffusione, riducono gli ostacoli della visibilità pubblica e inseriscono gli utenti in reti digitali globali organizzate. Basta uno smartphone per partecipare alla sfera pubblica digitale. Secondo: nella loro offerta informativa pubblica, le piattaforme non producono contenuti propri perché il loro modello commerciale si basa sulla diffusione di contenuti creati dagli utenti e non prevede un controllo redazionale (cosidd. *user-generated content*) da parte delle piattaforme. Terzo: i modelli economici delle piattaforme che determinano quali contenuti vengono messi in rilievo si basano sostanzialmente su un ampio raggio d'azione e sulla viralità, ossia sul fatto che gli utenti interagiscono il più possibile pubblicando contenuti, commentandoli, condividendoli oppure apponendovi un like. L'agenda tematica pubblica delle piattaforme è quindi plasmata dagli utenti stessi. Quarto: spesso gli utenti possono restare anonimi sulle piattaforme e partecipare al discorso pubblico senza dover rivelare la propria identità.

Queste caratteristiche delle piattaforme digitali non solo facilitano lo scambio pubblico e democratico tra gli individui ma favoriscono anche tutta una serie di fenomeni negativi, tra cui l'incitamento all'odio. Chiaramente sulle piattaforme non tutto è permesso. Se i contenuti violano le condizioni generali delle piattaforme, ne viene ridotta la visibilità o vengono rimossi. Le disposizioni delle singole piattaforme differiscono notevolmente soprattutto per quanto riguarda la libertà di espressione. I servizi come Gab o Telegram rinunciano ampiamente a una moderazione dei contenuti. La principale sfida delle piattaforme come Facebook o YouTube, che hanno regole interne più severe, è che i loro sistemi automatizzati devono essere in grado di rilevare e rimuovere in modo adeguato varie forme di discorsi di odio rivolti a diversi gruppi sociali e in più lingue. In molti casi ciò non avviene. Nel complesso l'anonimato, la portata delle reti di comunicazione digitali e il fatto che i relativi contenuti siano pubblici fanno sì che continuino ad esserci utenti presi di mira. Spesso però ai colpevoli vengono inflitte poche sanzioni, tanto meno di tipo legale. In definitiva, i discorsi di odio vietati offline rischiano di rimanere di fatto impuniti online.

Sul piano internazionale, i risultati mostrano chiaramente l'entità dell'incitamento all'odio sulle piattaforme digitali e i rischi sociali correlati. Circa la situazione in Svizzera sono disponibili pochi dati. Generalmente le piattaforme stesse pubblicano dati aggregati (globali) che non consentono di trarre conclusioni sulla situazione della Svizzera. Nemmeno le analisi specifiche dei Paesi nel quadro del codice di condotta dell'UE per contrastare i discorsi di odio illegali (*Code of conduct on countering illegal hate speech*) (cfr. cap. 3) sono indicative per quanto riguarda l'effettiva presenza dei discorsi di odio nei singoli Paesi. A causa della scarsità di ricerche in materia, nel 2021 e nel 2022 l'UFCOM ha

[5] https://www.bakom.admin.ch/bakom/it/pagina-iniziale/digitale-e-internet/comunicazione_digitale/piattaforme-di-comunicazione.html.

messo a concorso studi nel campo dell'incitamento all'odio digitale e nel frattempo sono disponibili i risultati della prima fase del progetto[6].

2.1 Reazioni politiche alla problematica dell'incitamento all'odio in Svizzera

Di recente in Svizzera diversi interventi parlamentari si sono occupati della diffusione dei discorsi di odio sulle piattaforme digitali, concentrandosi principalmente su tre aspetti. Siccome la portata dei discorsi di odio sulle piattaforme di social media non è chiara, la politica auspica una maggiore trasparenza da parte degli intermediari sul numero di casi che violano le loro condizioni di utilizzo e le basi legali vigenti in quest'ambito (cfr. cap. 4), nonché su quali siano i gruppi sociali prevalentemente coinvolti[7]. La maggior parte degli interventi parlamentari si concentra sulle misure e le possibilità normative che servono per arginare la problematica e rendere gli intermediari più responsabili[8]. Inoltre, le autorità dovrebbero essere in grado di sanzionare i discorsi di odio online. L'ultimo aspetto trattato riguarda sostanzialmente il ruolo dei Cantoni, ad esempio per quanto concerne la possibilità di denunciare i discorsi di odio e le questioni relative alla prevenzione[9].

2.2 Progetto di regolamentazione del Consiglio federale

Nel suo rapporto del 2022 su mozioni e postulati, nell'ambito della trattazione delle mozioni 18.3306 ("Rafforzare l'applicazione del diritto in Internet introducendo un recapito obbligatorio per le grandi piattaforme commerciali in rete") e 18.3379 ("Accesso delle autorità di perseguimento penale ai dati conservati all'estero") il Consiglio federale ha sottolineato che, una volta conclusi i lavori del Consiglio d'Europa relativi alla revisione della Convenzione sulla cibercriminalità, analizzerà il valore aggiunto e la necessità di attuazione in Svizzera[10].

In seguito alla pubblicazione del rapporto dell'Ufficio federale delle comunicazioni UFCOM in collaborazione con la Cancelleria federale "Intermediari e piattaforme di comunicazione. Effetti sulla comunicazione pubblica e approcci di governance" e sulla base del documento di discussione, il 5 aprile 2023 il Consiglio federale ha incaricato il DATEC (UFCOM) di preparare un progetto da porre in consultazione sulla regolamentazione delle piattaforme di comunicazione.

---

[6] Gli studi pubblicati finora sono disponibili sul sito Internet dell'UFCOM: https://www.bakom.admin.ch/bakom/it/pagina-iniziale/media-elettronici/studi/le-singole-analisi.html

Nel quadro del bando dettagliato 2022 l'UFCOM sostiene cinque progetti che analizzano ad esempio la frequenza dei discorsi di odio sulle piattaforme digitali, la consapevolezza degli utenti, come gli algoritmi possono individuare tali discorsi e definire quali gruppi sociali sono maggiormente colpiti. Sono inoltre identificate le possibilità (normative) esistenti per contrastare l'incitamento all'odio.

[7] Ip. 17.3751, Ip. 19.3255, Dmd. 20.5670, Po. 21.4531, Po. 22.3201.

[8] Ip. 14.3888, Ip. 17.3751, Ip. 17.3734, Ip. 19.3255, Ip. 19.3787, Ip 20.3686, Ip. 20.5670, Ip. 21.3123, Ip. 21.3684, Ip. 21.4532, Ip. 22.3156, Ip. 22.3157, Ip. 22.3305, Ip. 21.3683, Mo. 16.4082, Mo. 18.3306, Mo.18.3379, Mo. 20.4357, Iv. Pa. 13.407, Iv. Pa. 20.445, Iv. Pa. 21.524, Iv. Pa. 21.525, Po. 11.3912, Po. 22.3201, Po. 21.3969. Tra questi rientrano estensioni di fattispecie penali esistenti, ad es. per includere la caratteristica del genere nell'ambito di protezione dell'art. 261bis CP (cfr. le sei iniziative parlamentari di tenore identico 21.513, 21.514, 21.515, 21.516, 21.522, 21.527 "Gli incitamenti all'odio e alla violenza a motivo del sesso devono essere punibili").

[9] Ip. 20.3686, Ip. 21.3123, Ip. 22.3156, Ip. 22.3305, Po. 22.3201.

[10] www.bk.admin.ch > *Documentazione* > Aiuto alla condotta strategica > *Rapporto mozioni e postulati* > *Archivio*

3 Approcci normativi internazionali

La legislazione sui discorsi di odio deve sempre rendere giustizia a due diritti umani strettamente correlati che sono in tensione tra loro: la libertà di espressione e la protezione contro la discriminazione. L'attività legislativa svizzera in materia di discorsi di odio è integrata in norme e obblighi internazionali. Di primaria importanza sono l'Organizzazione delle Nazioni Unite (ONU) e le sue sotto-organizzazioni, il Consiglio d'Europa e i suoi organi e, soprattutto nella sfera digitale, gli attuali sforzi normativi profusi dall'Unione europea (UE) e da singoli Stati europei. In diversi Paesi europei e nell'UE si è affermata l'idea che il quadro giuridico esistente non basti a contenere i discorsi e la propaganda di odio online in quanto risale a un'epoca analogica e non è più in grado di tenere sufficientemente conto delle mutate condizioni digitali.

Tra le misure legali contro i discorsi di odio digitali figura in prima linea il *Digital Services Act* (DSA) dell'UE, entrato in vigore il 16 novembre 2022[11]. Seguendo il principio secondo cui ciò che è punibile offline deve esserlo anche online, il DSA formula tutta una serie di obblighi di diligenza nei confronti delle piattaforme digitali. Ai grandi intermediari attivi a livello globale impone ulteriori obblighi di trasparenza e rendiconto. Tuttavia, il DSA affida agli intermediari la progettazione concreta della moderazione dei contenuti incaricandoli praticamente di formulare regole determinati, che esplicano effetti simili a quelli del diritto statale. Gli organismi ufficiali a loro volta sorvegliano, tramite un controllo della qualità, l'efficacia della moderazione dei contenuti da parte degli intermediari. Per quanto riguarda i discorsi di odio il DSA è affiancato dall'*EU Code of conduct on countering illegal hate speech online*, un approccio volontario di autoregolamentazione sottoscritto, tra gli altri, da Facebook, X, Instagram e YouTube. La sua efficacia viene regolarmente verificata e, dopo un'attenta valutazione, è stata giudicata insufficiente dall'UE. L'inserimento dell'accordo di settore nel quadro di co-regolamentazione del DSA dovrebbe ora contribuire a uniformare gli obblighi di rendiconto degli intermediari. Vi si aggiungono altre raccomandazioni della Commissione europea che non hanno tuttavia valore legale vincolante[12].

In vista di queste iniziative, alcuni Stati europei hanno creato basi legali proprie per responsabilizzare hmaggiormente le (grandi) piattaforme digitali nella lotta contro i discorsi di odio. Pur avendo orientamenti diversi, le varie leggi (*Netzwerkdurchsetzungsgesetz* in Germania, *Kommunikationsplattformgesetz* in Austria, *Online Safety Bill* nel Regno Unito o la *Loi visant à lutter contre les contenus haineux sur internet* in Francia) perseguono un obiettivo comune, ossia la protezione della popolazione, in particolare dei bambini e dei giovani, la sicurezza nazionale e la tutela dei diritti fondamentali in generale[13]. Attraverso la loro legislazione, singoli Stati, come la Germania e l'Austria, mirano esplicitamente a una migliore applicazione del diritto penale nei confronti degli intermediari digitali.

[11] COMMISSIONE EUROPEA (19.10.2022), Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali, GU L 277 del 27.10.2022, pagg. 1-102).

[12] COMMISSIONE EUROPEA (01.03.2018), Raccomandazione (UE) 2018/334 della Commissione, del 1° marzo 2018, sulle misure per contrastare efficacemente i contenuti illegali online, GU L 63 del 6.3.2018, pagg. 50-61; COMMISSIONE EUROPEA (2017), Lotta ai contenuti illeciti online Verso una maggiore responsabilizzazione delle piattaforme online. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni COM(2017) 555.

[13] BUNDESTAG TEDESCO (2017), Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz NetzDG); ÖSTERREICHISCHER NATIONALRAT (2021), Bundesgesetz über Massnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-Gesetz – KoPl-G); DEPARTMENT FOR DIGITAL, CULTURE, MEDIA AND SPORT (2022), A Bill to make provision for and in connection with the regulation by OFCOM of certain internet services; for and in connection with communications offences; and for connected purposes (Online Safety Bill); ASSEMBLÉE NATIONALE (FRANCIA) (25.06.2020), LOI n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet.

4 Analisi giuridica

Le sezioni seguenti presentano le attuali possibilità di affrontare il discorso di odio dal punto di vista delle varie aree del diritto, evidenziando anche le sfide esistenti. I sottocapitoli successivi illustrano le possibilità e le sfide legali specifiche sul piano del diritto penale (cap. **Fehler! Verweisquelle konnte nicht gefunden werden.**), delle misure preventive di polizia (cap. 4.4.1) nonché di altre disposizioni di diritto pubblico (cap. 4.4.2). L'analisi è completata da un excursus sul diritto civile (cap. 4.3). Le spiegazioni delle singole aree del diritto sono precedute da alcune osservazioni introduttive sulla natura particolare del discorso di odio online.

4.1 Particolarità del discorso di odio online

Il principio di territorialità stabilisce che tutte le persone che si trovano sul territorio svizzero soggiacciono alle leggi svizzere. Questo vale anche per lo spazio digitale. Secondo la giurisprudenza del Tribunale federale, chi tramite Internet in Svizzera accede a un servizio offerto da una società straniera non agisce "all'estero" (principio dell'accesso)[14]. Agli utenti delle piattaforme digitali si applicano infatti le leggi svizzere anche se tali piattaforme hanno la loro sede principale all'estero.

Se i dati si trovano in Svizzera, le autorità di persecuzione penale possono *ingiungere all'obbligato di procedere alla consegna* (art. 265 CPP, cfr. anche art. 264 CPP), *perquisire i sistemi informatici di privati* (art. 246 CPP) e *sequestrare* i dati o i *supporti di dati*, come smartphone o laptop (art. 263 e segg. CPP)[15]. Naturalmente, ciò presuppone che il proprietario possa essere identificato senza ombra di dubbio. Questo può essere un problema per i profili e gli account sulle piattaforme digitali, che spesso sono anonimi.

L'*obbligo di conservare i dati sul traffico Internet* non è regolamentato in modo uniforme e dipende in larga misura dalla questione se l'operatore del server rientri nell'ambito di applicazione della legge federale del 18 marzo 2016 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT; RS 780.1).

Secondo la giurisprudenza del Tribunale federale, le filiali svizzere di Alphabet (Google) e Meta (Facebook/Instagram) non sono proprietarie dei dati degli utenti, poiché si limitano a commercializzare i servizi ma non li gestiscono[16]. I dipendenti di tali aziende non sono quindi obbligati a collaborare in tal senso. Per procurarsi i dati non conservati in Svizzera, le autorità di perseguimento penale devono quindi ricorrere all'assistenza giudiziaria (cfr. cap. 4.2.3.2). La problematica della persecuzione penale aggravata viene descritta al capitolo **Fehler! Verweisquelle konnte nicht gefunden werden.** e può essere consultata nel dettaglio nel rapporto del Consiglio federale "Completare il Codice penale con disposizioni concernenti il ciberbullismo"[17].

4.2 Analisi alla luce del diritto penale

Il diritto penale svizzero non riconosce un reato che consiste nel discorso di odio. Tuttavia, a seconda della situazione concreta, potrebbero essere applicate diverse disposizioni del Codice penale svizzero del 21 dicembre 1937 (CP; RS 311.0), come mostra la seguente analisi.

4.2.1 Opzioni a livello di diritto penale

A seconda della tipologia del caso, tra le fattispecie penali rientrano in particolare:

- l'articolo 135 CP (rappresentazioni di atti di cruda violenza);
- gli articoli 173 e seguenti CP (delitti contro l'onore);

[14] DTF 143 IV 270, 287 segg.

[15] Il detentore può chiedere l'apposizione di sigilli ai dati, tuttavia, il Tribunale federale stabilisce requisiti relativamente elevati per la rivendicazione dell'interesse al mantenimento del segreto.

[16] DTF 143 IV 21, 25 seg. e sentenza del TF 1B_142/2016 del 16.11.2016, consid. 3.

[17] Disponibile all'indirizzo: https://www.newsd.admin.ch/newsd/message/attachments/73646.pdf.

- l'articolo 180 CP (minaccia);
- l'articolo 181 CP (coazione) e
- l'articolo 258 e seguenti CP (dei crimini o dei delitti contro la tranquillità pubblica).

All'interno di quest'ultimo gruppo sono particolarmente degni di nota l'articolo 259 CP (pubblica istigazione a un crimine o alla violenza) e l'articolo 261bis CP (discriminazione e incitamento all'odio). Quest'ultima disposizione si applica se il discorso di odio contiene i seguenti elementi: incitamento pubblico all'odio o alla discriminazione contro una persona o un gruppo di persone per la loro razza, etnia, religione o per il loro orientamento sessuale (cpv. 1), propagazione di tali ideologie (cpv. 2), partecipazione, organizzazione e incoraggiamento di azioni di propaganda corrispondenti (cpv. 3), nonché il discreditare e discriminare in modo lesivo della dignità umana a causa della razza, etnia, religione o orientamento sessuale o il disconoscere, minimizzare grossolanamente o cercare di giustificare il genocidio o altri crimini contro l'umanità per i suddetti motivi mediante parole, scritti, immagini, gesti, vie di fatto o in altro modo (cpv. 4)[18]. Questa fattispecie legale protegge la dignità umana e (in via accessoria) la tranquillità pubblica dichiarando punibile l'incitamento all'odio e la discriminazione pubblici quando prendono di mira determinate caratteristiche essenziali della personalità.

Dal punto di vista del diritto penale, il discorso di odio online si differenzia da quello offline solo perché viene commesso utilizzando le tecnologie dell'informazione e della comunicazione (TIC). Pertanto, tutte le disposizioni penali di cui sopra sono applicabili anche ai reati online.

4.2.2 Responsabilità penali nello spazio online

Le persone che in un procedimento penale, nonostante l'ingiunzione, nascondono alle autorità dati necessari a fini probatori sono perseguibili penalmente (art. 265 cpv. 3 CPP)[19]. Chiunque violi un obbligo di cooperazione nell'ambito della procedura penale può essere punito per disobbedienza a decisioni dell'autorità (art. 292 CP). Una disposizione speciale analoga si applica alle persone che hanno l'obbligo di collaborare ai sensi della LSCPT[20] (art. 39 cpv. 1 lett. a LSCPT).

Può essere fondamentalmente punito per complicità al reato principale dell'utente, chiunque fornisca l'infrastruttura tecnica con cui l'utente commette un reato (art. 25 CP). Sulla base della prassi giudiziaria esistente, si potrebbe quindi aprire un procedimento penale per complicità contro il direttore generale di una piattaforma di social media estera che non è disposto a collaborare nel caso di un reato di opinione commesso da un utente della piattaforma.

Inoltre, in applicazione della responsabilità a cascata, se un reato di opinione viene commesso attraverso una piattaforma di social media, può essere chiamata in causa la punibilità del gestore della piattaforma in base al diritto penale dei media[21]. Se l'autore di una pubblicazione su una piattaforma non può essere identificato, la persona responsabile della piattaforma può essere punita secondo le norme del diritto penale dei media per non aver impedito, intenzionalmente o per negligenza, una pubblicazione punibile (art. 28 CP).

In presenza di una decisione passata in giudicato, il contenuto illegale[22] deve essere rimosso da Internet. Tuttavia, la rimozione risulta difficile o addirittura impossibile se il provider ha sede

[18] Il sesso di una persona o la sua identità sessuale attualmente non sono protetti dall'articolo 261bis CP (v. nota 7).

[19] L'imputato non è tenuto a collaborare (principio nemo tenetur, art. 113 CPP); anche la facoltà di non deporre può costituire un'eccezione, cfr. art. 264 seg. CPP.

[20] In particolare i fornitori di servizi di telecomunicazione (FST), ma anche chi mette a disposizione indirizzi e-mail, i gestori delle piattaforme, ecc.

[21] TRECHSEL/JEAN-RICHARD, CP art. 28 N 14. Il diritto dell'UE esclude un obbligo generale di vigilanza. In Svizzera, il Tribunale federale non ha mai dovuto giudicare la responsabilità dei gestori di piattaforme in quanto media ai sensi dell'art. 28 CP.

[22] Ad es. pornografia, violazione dell'onore, discriminazione razziale.

all'estero e se sia lui che l'autore del reato si rifiutano di collaborare. Per questo motivo, si sta valutando la possibilità di imporre ordini di blocco ai fornitori di accesso in Svizzera, al fine di bloccare i contenuti Internet per il pubblico svizzero. In pratica, tuttavia, queste misure sono solo parzialmente efficaci, in quanto possono essere aggirate con relativa facilità.

4.2.3 Sfide inerenti al diritto penale

Quanto detto sopra riguardo alle disposizioni del diritto penale dimostra che il diritto materiale fornisce in linea di principio un insieme differenziato di strumenti per iscrivere i discorsi di odio nel diritto penale. È però problematico il fatto che tali atti siano spesso commessi da autori anonimi. L'identificazione degli autori e la ricerca delle prove e il metterle al sicuro sulle piattaforme digitali rappresentano pertanto una sfida particolare. Le difficoltà non risiedono quindi tanto nel diritto materiale in sé, quanto piuttosto nell'applicazione della legge.

4.2.3.1 Limiti nel Codice penale: violazione della sovranità territoriale di uno Stato estero

Secondo il diritto svizzero, un'azione diretta delle autorità di perseguimento penale svizzere è in linea di principio inaccettabile in quanto, trasgredendo le disposizioni di assistenza giudiziaria internazionale in materia penale, avverrebbe una violazione della sovranità territoriale di uno Stato estero ed eventualmente le prove raccolte non potrebbero essere utilizzate. Va inoltre tenuto presente che il compimento di un atto ufficiale può essere punito anche in base al diritto estero. Sebbene gli Stati Uniti consentano alle autorità di perseguimento penale svizzere di richiedere direttamente ai fornitori di servizi Internet di assicurare e consegnare i dati, questi ultimi spesso non soddisfano tali richieste. Pertanto, l'assistenza giudiziaria è di fondamentale importanza per l'ottenimento di dati all'estero.

4.2.3.2 Assistenza giudiziaria

Nel caso dell'assistenza giudiziaria, le misure di indagine penale vengono eseguite in uno Stato estero su richiesta di un altro Stato analogamente ai procedimenti penali propri - soltanto che le prove raccolte sono utilizzate in un procedimento penale estero (nello Stato a cui è stata chiesta l'assistenza giudiziaria). Le basi giuridiche provengono generalmente dal diritto internazionale[23] o dal diritto amministrativo. La procedura è retta dalla legge federale del 20 marzo 1981 sull'assistenza internazionale in materia penale (AIMP; RS 351.1). Le procedure di assistenza giudiziaria richiedono molto tempo e, a seconda dei casi, possono passare diversi mesi prima che le autorità di perseguimento penale ottengano i dati. A seconda dell'ordinamento giuridico straniero, inoltre, non è previsto salvaguardare o bloccare immediatamente i dati a titolo provvisorio, il che complica ulteriormente il lavoro delle autorità di perseguimento penale. La via dell'assistenza giudiziaria può essere lunga e onerosa[24].

Questo è dovuto a diversi fattori. La maggior parte degli operatori di piattaforme, soprattutto quelli di grandi dimensioni, ha sede negli Stati Uniti. Il controllo sui dati è spesso rivendicato dalle loro sedi principali, motivo per cui la raccolta di prove tramite l'assistenza giudiziaria viene spesso effettuata sulla base del Trattato conchiuso il 25 maggio 1973 con gli Stati Uniti d'America sull'assistenza giudiziaria in materia penale (TAGSU; RS 0.351.933.6). Un presupposto fondamentale per ordinare in modo obbligatorio la raccolta di prove/l'assunzione di prove è la doppia punibilità (art. 4 n. 2 TAGSU). Questa è data se il reato è punibile sia in base alla legge svizzera che alla legge statunitense. Il reato deve inoltre figurare nell'elenco dei reati per i quali possono essere applicate misure coercitive ai sensi del trattato bilaterale. A prescindere dalla responsabilità penale secondo la legge statunitense per i delitti contro l'onore (art. 173 e segg. CP) ma anche per i reati contro il divieto di discriminazione razziale (art. 261bis CP), le richieste di assistenza giudiziaria indirizzate agli Stati Uniti per tali reati non vengono soddisfatte, facendo riferimento alla libertà di espressione garantita dal primo Emendamento della Costituzione statunitense. Di conseguenza, per questo tipo di reati non sussiste nei confronti degli Stati Uniti il diritto di ricorrere a misure coercitive tramite l'assistenza giudiziaria.

I gestori delle piattaforme prevedono la consegna dei dati esclusivamente sulla base di un ordine giudiziario, il quale non può essere emesso secondo la legge statunitense.

[23] Trattati statali multilaterali o bilaterali.

[24] Cfr. SIEBER/NEUBERT, pag. 246.

Per richiedere l'assistenza giudiziaria agli Stati europei valgono considerazioni analoghe. Sebbene molti di essi pongano limiti più ristretti alla libertà di espressione rispetto agli Stati Uniti, anche in questo caso le singole dichiarazioni devono essere soppesate rispetto alle nozioni di libertà civile o al diritto penale applicabile. Inoltre, poiché i reati di incitamento all'odio sono in molti casi classificati come reati minori e l'azione penale è complessa, anche in Europa l'accesso ai dati da parte delle autorità svizzere è possibile solo in misura limitata. A differenza degli Stati dell'EFTA Norvegia e Islanda, la Svizzera non prende parte agli approcci più ampi dell'UE, che rendono superflua la verifica della responsabilità penale reciproca.

4.3 Excursus: strumenti di diritto privato

Una persona vittima di discorsi di odio o di altre forme di attacchi digitali è di solito illecitamente lesa nella sua personalità. A sua tutela, può quindi chiedere l'intervento del giudice contro chiunque partecipi all'offesa (art. 28 cpv. 1 CC). In questo modo, l'interessato può chiedere di proibire una lesione imminente o di far cessare una lesione attuale (art. 28a cpv. 1 n. 1 e 2 CC). Questa regolamentazione è tecnologicamente neutra. È quindi ipotizzabile che, su tale base, vengano ordinati sia la cancellazione che il blocco dei contenuti illegali su Internet.

Diversamente dal diritto penale, secondo le regole generali della procedura civile, il ricorrente, ossia in questo caso la vittima di un discorso di odio, deve dimostrare in tribunale di essere stato illegittimamente violato nella sua personalità da una certa persona. Nei casi in cui l'utente autore della violazione non è noto, la possibilità di intraprendere un'azione contro i complici è di grande importanza. Pertanto nel rapporto "La responsabilità civile dei provider" dell'11 dicembre 2015, il Consiglio federale ha tra l'altro esaminato la possibilità di intraprendere azioni di soppressione dello stato di fatto nei confronti di vari attori di Internet [25].

Al fine di garantire la tutela giuridica delle persone interessate, conformemente alle basi giuridiche generali è possibile e, secondo il Consiglio federale, anche auspicabile che, tenendo conto del principio di proporzionalità, i fornitori di contenuti come i gestori delle piattaforme di social media possano essere obbligati a rimuovere i contenuti illeciti.

4.3.1 Sfide a livello di diritto privato

Far valere i diritti all'estero è spesso associato a difficoltà anche nel campo del diritto privato. Nel corso della preparazione del suddetto rapporto, è stata esaminata in modo approfondito la possibilità di obbligare alcuni fornitori a designare un domicilio per le notifiche in Svizzera, al fine di facilitare l'applicazione del diritto civile nei loro confronti. In questo rapporto, il Consiglio federale è giunto alla conclusione che la questione del domicilio di notifica nel diritto civile non dovrebbe essere perseguita in via prioritaria per il momento. Si dovrebbe piuttosto promuovere la conclusione di accordi di assistenza giudiziaria reciproca o di accordi che prevedano la notifica diretta a mezzo posta di documenti in materia civile. La possibilità di un recapito postale diretto esiste già oggi per alcuni Stati in cui hanno sede legale noti operatori di piattaforme[26].

Se una decisione è stata emessa ma la parte convenuta non vi si adegua volontariamente, occorre procedere all'esecuzione, nei casi transfrontalieri ciò comporta comunque uno sforzo considerevole. Negli Stati membri della Convenzione di Lugano (CLug; RS 0.275.12) la parte lesa può, con la sua sentenza svizzera, rivolgersi direttamente all'autorità esecutiva dello Stato in questione. Se una decisione svizzera deve essere applicata al di fuori dell'area UE/AELS, ad esempio perché il provider è domiciliato nel luogo in questione, la sua riconoscibilità dipende solitamente dal diritto interno del rispettivo Stato [27]. Se si prevedono difficoltà in tal senso, la persona danneggiata è costretta a intentare una nuova causa nello Stato in questione o a presentarla direttamente nello Stato estero. La legge che disciplina la responsabilità del fornitore in un caso specifico è quindi determinata dalle norme di

[25] Rapporto del Consiglio federale "Responsabilità civile dei provider" dell'11 dicembre 2015, disponibile in tedesco e francese all'indirizzo: https://www.bj.admin.ch/dam/bj/fr/data/publiservice/publikationen/berichte-gutachten/berichte/verantwortlichkeit-provider/ber-br.pdf.download.pdf/ber-br-f.pdf.

[26] USA, Irlanda, cfr. Rapporto del Consiglio federale "Responsabilità civile dei provider", n. 6.2.4.

[27] Rapporto del Consiglio federale "Responsabilità civile dei provider" (n. **Fehler! Textmarke nicht definiert.**), n. 6.2.5.

quello Stato. La necessità di attuare la legge all'estero può talvolta comportare grandi difficoltà pratiche e ritardi nella rimozione dei contenuti illegali[28].

Vi sono solo poche sentenze del Tribunale federale concernenti complicità alla violazione dei diritti della personalità su Internet. Queste riguardano i portali di media svizzeri[29]. Sul perché non siano note sentenze riguardanti piattaforme estere, si possono avanzare solo ipotesi. Molto probabilmente l'esecuzione transfrontaliera delle azioni civili è considerata troppo onerosa e lunga.

4.4 Diritto pubblico

Negli ambiti di diritto pubblico, a differenza del diritto privato, in linea di principio è lo Stato da solo a garantire il rispetto della legge. Ciò include ad esempio misure preventive di polizia (v. cap. 4.4.1). Nel settore radiotelevisivo è invece l'UFCOM a vigilare sul rispetto della legge federale sulla radiotelevisione (LRTV; RS 784.40), dell'ordinanza sulla radiotelevisione (ORTV; RS 784.401) e degli accordi internazionali pertinenti (v. cap. 4.4.2.1).

4.4.1 Aspetti preventivi di polizia

Le misure preventive di polizia della Confederazione contro il discorso di odio comprendono in particolare la messa al sicuro, il sequestro e la confisca di materiale di propaganda con contenuti tesi a istigare violenza, e la protezione delle autorità e degli edifici della Confederazione. Nel settore online alcuni intermediari dispongono inoltre dei cosiddetti programmi "trusted flagger" che trattano in modo prioritario le segnalazioni provenienti da istituzioni registrate, come fedpol[30].

4.4.1.1 Materiale di propaganda

Gran parte delle misure per combattere la propaganda di odio hanno come fondamento la legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI; RS 120). Questa offre in particolare la possibilità di intraprendere azioni preventive contro la violenza, l'incitamento alla violenza e le attività terroristiche, permettendo anche di contrastare i discorsi e la propaganda di odio. Sulla base dell'articolo 13*e* LMSI le autorità di polizia e doganali possono mettere al sicuro materiale che può servire a scopi propagandistici. Anche il personale competente del Servizio delle attività informative della Confederazione (SIC) o di fedpol, se si imbatte in tale materiale, può a sua volta sequestrarlo.

In caso di diffusione di propaganda di odio terroristico, le autorità competenti possono adottare per tempo misure specifiche contro le persone da cui proviene la relativa minaccia. Nel caso di tentativi di radicalizzazione di terzi attraverso la propaganda di odio terroristico, viene preso in considerazione soprattutto il divieto di avere contatti (art. 23*l* LMSI). Vi è anche una questione di inclusione o esclusione (art. 23*m* LMSI), tramite cui si può impedire a un potenziale terrorista di rimanere in determinati luoghi. Se una persona divulga ideologie di odio terrorista, va inoltre considerato l'obbligo di presentarsi e di partecipare a colloqui (art. 23*k* LMSI). Fedpol può ordinare queste misure caso per caso su richiesta dei Cantoni, eventualmente dei Comuni, o del Servizio delle attività informative della Confederazione (SIC). Sono sempre sussidiarie e complementari alle misure sociali, integrative o terapeutiche, nonché sussidiarie alle misure di prevenzione generale delle minacce adottate dai Cantoni e alle misure di procedura penale (art. 23*f* LMSI).

---

[28] Cfr. il contributo di *Schneider-Marfels*, Jusletter 20 febbraio 2012 relativo a un ordine super provvisorio contro Facebook (in tedesco).

[29] Cfr. DTF 147 III 185 (Blick.ch), sentenza del TF 5A_792/2011 del 14 gennaio 2013 (Tribune de Genève).

[30] Da novembre 2016 a novembre 2020, fedpol ha segnalato 365 video su YouTube, la maggior parte dei quali (311) sono stati limitati o rimossi. Secondo le stime di fedpol, almeno il 90% dei video segnalati riguardava contenuti di terrorismo e relative rappresentazioni di atti di violenza. Le restanti segnalazioni riguardavano ad es. video di suicidi, crudeltà verso gli animali, video di sextortion e video con contenuti razzisti. Negli anni precedenti, fedpol non ha effettuato alcuna segnalazione perché non è stato possibile trovare contenuti per cui richiedere la soppressione. fedpol agisce di propria iniziativa, spesso anche sulla base di segnalazioni di contenuti illegali da parte della popolazione.

Se con la diffusione di propaganda di odio estremista violenta o terroristica una persona straniera mette in pericolo la sicurezza interna o esterna della Svizzera, fedpol può decidere misure in materia di diritto degli stranieri (divieto d'entrata, espulsione) sulla base dell'articolo 67 capoverso 4 e dell'articolo 68 della legge del 16 dicembre 2005 sugli stranieri e la loro integrazione (LStrI; RS *142.20*).

In base al diritto in materia di polizia esistono possibilità d'intervento della polizia. Si pensi a un ordine di allontanamento nel caso di discorsi di odio punibili diffusi in luoghi pubblici. Se delle persone diffondono discorsi di odio, entra eventualmente in azione il sistema cantonale di gestione delle minacce per identificare, valutare e neutralizzare per tempo il pericolo potenziale rappresentato da singole persone.

4.4.1.2 Protezione delle autorità e degli edifici della Confederazione

In collaborazione con le autorità cantonali, fedpol assicura la protezione delle autorità e degli edifici della Confederazione nonché delle persone e degli edifici di cui la Confederazione deve garantire la sicurezza in virtù di obblighi di diritto internazionale pubblico (art. 22 LMSI). Per adempiere questo mandato, fedpol interviene a titolo consultivo od ordina le misure di polizia necessarie se le persone che devono essere protette dalla Confederazione sono messe in pericolo da discorsi di odio o minacce. Qualora sussistano motivi concreti per presumere che una determinata persona commetterà un reato, fedpol e le autorità cantonali di polizia da questo incaricate possono in particolare condurre colloqui con le persone pericolose (art. 23 cpv. 3bis LMSI in combinato disposto con l'art. 14 OPCF; RS 120.72).

4.4.1.3 Settore online

Imprese come Alphabet (Google), Meta (Facebook, Instagram) e X offrono le cosiddette procedure di notifica e soppressione che consentono agli utenti di segnalare le violazioni dei diritti nei vari Paesi. In seguito a ciò gli intermediari controllano i contenuti e successivamente, se necessario, li bloccano[31] o eliminano. Alcune piattaforme riservano un trattamento privilegiato alle segnalazioni provenienti da determinate istituzioni. Un esempio noto è il programma "Priority Flagger" di YouTube. Un priorityflagger è un utente particolarmente affidabile alle cui segnalazioni e allerte l'impresa reagisce più rapidamente rispetto agli utenti ordinari. Fedpol ha lo stato di un priority flagger presso YouTube e intrattiene contatti con X e Facebook.

Se viene diffuso materiale di propaganda violenta via Internet, fedpol può ordinare la soppressione del sito web in questione sulla base dell'articolo 13*e* LMSI (dopo aver consultato il Servizio delle attività informative della Confederazione SIC), se il materiale di propaganda si trova su un computer svizzero. In caso contrario, fedpol può comunque raccomandare al provider svizzero di bloccare la pagina web in questione. È inoltre possibile revocare un nome di dominio svizzero se viene usato per diffondere materiale di propaganda violenta[32].

4.4.1.4 Sfide e lacune nelle misure preventive di polizia

La diffusione di discorsi di odio, soprattutto via Internet, è un problema in aumento. I discorsi di odio possono causare o rafforzare processi di radicalizzazione e portare alla violenza fisica, anche se gli autori stessi non intraprendono alcuna azione. L'odio e le minacce sono talvolta rivolti anche ai politici, il che può indurli a ritirarsi dal dibattito politico pubblico. Inoltre, i discorsi di odio scoraggiano determinate persone ad assumere certe funzioni politiche perché non vogliono esporsi a pericoli o ai discorsi di odio. Pertanto questi discorsi non minacciano solo le persone, bensì anche le istituzioni e il discorso democratico.

4.4.1.4.1 Diffusione di discorsi di odio tramite piattaforme Internet

[31] Nel senso di geo-blocking (blocco dei contenuti per determinate regioni).

[32] La legge sulle telecomunicazioni disciplina la procedura con cui fedpol può ordinare la revoca di un nome di dominio (v. cap. 4.4.2.4).

La Svizzera non conosce procedure generali di segnalazione e rimedio ("notice and action"), come quelle introdotte dal DSA. L'obbligo per un intermediario di controllare, sulla base delle segnalazioni delle autorità svizzere, ed eventualmente di rimuovere i contenuti viene valutato in base alle disposizioni generali del diritto civile e penale. Le autorità di polizia non hanno nemmeno la possibilità di esigere che i servizi digitali sopprimano i discorsi di odio illegali (v. cap. 4.4.1.3).

Attualmente gli operatori delle piattaforme non sono obbligati per legge a segnalare alla polizia e alle altre autorità di perseguimento penale i contenuti illegali o di sopprimerli anche se hanno indizi di un reato (grave)[33].

4.4.1.4.2 Materiale di propaganda

In base all'articolo 13*e* del LMSI, fedpol può intervenire solo contro materiale di propaganda il cui contenuto incita *concretamente* e *seriamente* alla violenza contro persone o cose. L'articolo 13*e* LMSI non prende in considerazione il contesto di utilizzo di determinati simboli. Sul piano del diritto in materia di prevenzione dei rischi, non è molto avveduto tollerare l'importazione e la diffusione ad esempio di simboli nazisti o dell'IS (che non incitano direttamente alla violenza) se, considerate le circostanze concrete, ci si deve seriamente aspettare che saranno utilizzati per scopi criminali, come il sostegno a organizzazioni terroristiche (art. 260ter CP), la discriminazione o l'incitamento all'odio (art. 261bis CP) o la pubblica istigazione a un crimine o alla violenza (art. 259 CP).

4.4.1.4.3 Scambio di informazioni

Le autorità cantonali di polizia non hanno modo di scambiarsi sistematicamente informazioni di polizia tra di loro. L'accesso è possibile solo su richiesta specifica in casi particolari, poiché non esiste una piattaforma nazionale di interrogazione della polizia attraverso cui le autorità con accesso autorizzato possano consultare i sistemi informativi della polizia presso la Confederazione, i Cantoni e quelli esteri tramite un'unica interrogazione[34].

4.4.1.4.4 Gestione delle minacce

La gestione delle minacce, in cui vengono analizzate informazioni pubbliche e non pubbliche provenienti dai sistemi federali e cantonali, presenta diverse lacune. Manca una base giuridica per un'analisi automatizzata dei dati e per la creazione di profili ad alto rischio per le persone coinvolte, al fine di effettuare una valutazione tempestiva della situazione e del rischio. Inoltre, l'attuale base giuridica non prevede diritti di accesso per le autorità cantonali ai dati di fedpol sulla gestione delle minacce e viceversa. Per garantire che le informazioni derivanti dall'attività di analisi possano essere utilizzate anche per eventuali procedure penali, ad esempio in caso di minaccia, è necessario regolamentare anche i diritti di accesso a questi dati da parte dei servizi di fedpol responsabili delle procedure di polizia giudiziaria.

4.4.2 Altre norme di diritto pubblico in vigore

Lo Stato è obbligato a prendere misure per garantire l'esercizio effettivo dei diritti fondamentali, in particolare quando tale esercizio è minacciato da altri attori[35]. L'effettiva tutela dei beni giuridici deve essere garantita sia offline che online. Questo vale per il diritto all'integrità fisica e psicologica dai discorsi di odio ma anche per i diritti fondamentali di comunicazione (libertà di opinione e d'informazione).

---

[33] Esiste un'eccezione nell'ambito della legge sulle telecomunicazioni per i contenuti pornografici ai sensi dell'art. 197 cpv. 4 e 5 CP.

[34] Questa lacuna è tematizzata dalla mozione 18.3592 "Scambio di dati di polizia su scala nazionale", adottata dal Consiglio nazionale e dal Consiglio degli Stati nel 2019; la sua attuazione è ora affidata al Consiglio federale.

[35] Cfr. in particolare Waldmann, BSK BV, art. 35 Cost, n. marg. 6 e 40.

4.4.2.1 Legge federale sulla radiotelevisione

La legge federale sulla radiotelevisione (LRTV) disciplina la diffusione, la preparazione tecnica, la trasmissione e la ricezione di programmi radiotelevisivi in Svizzera. La LRTV è stata concepita in modo da essere neutrale sul piano tecnologico poiché il suo campo di applicazione non dipende dal tipo di diffusione (Internet/radiodiffusione, linee/radiocomunicazione). Ciò significa che in linea di massima vi rientrano anche le emittenti di radio web e le televisioni Internet.

Nell'ambito del diritto dei media, l'articolo 4 capoverso 1 della LRTV è l'unica disposizione di legge che tratta esplicitamente il fenomeno del discorso di odio. Tuttavia, la disposizione si applica solo ai programmi radiotelevisivi svizzeri e all'ulteriore offerta editoriale della SSR. Per gli altri media giornalistici (ad es. la stampa e le piattaforme online di gruppi mediatici) in Svizzera non si applicano disposizioni legali speciali per quanto riguarda il contenuto delle pubblicazioni. Come spiegato nei capitoli 4.2 e 4.3, il diritto svizzero in vigore contiene però numerose disposizioni che proteggono dall'incitamento all'odio e possono essere considerate sufficienti a tal fine. Infatti, a differenza di quanto avviene ad esempio per i discorsi di odio digitali su piattaforme transnazionali, non ci sono problemi di applicazione della legge per i media con sede in Svizzera.

Inoltre il settore dei media svizzeri ha definito le proprie regole di condotta professionale. Con queste i mass media giornalistici si impegnano ad esempio ad attenersi alla verità, a rispettare la dignità umana e ad astenersi da allusioni discriminatorie[36]. Il Consiglio svizzero della stampa è tenuto a vigilare sulle regole di condotta professionale del settore dei media svizzeri. In quanto organo di autoregolamentazione ha ricordato in una presa di posizione che i doveri del codice dei giornalisti vanno presi in considerazione anche quando si trattano lettere alla redazione o commenti online[37].

Le emittenti radiotelevisive estere ci confrontano con ulteriori sfide perché il campo di applicazione della LRTV si estende soltanto alle emittenti svizzere. Tuttavia, la Svizzera è vincolata dalla Convenzione europea del 5 maggio 1989 sulla televisione transfrontaliera (CETT; RS 0.784.405). Questa, come l'articolo 4 capoverso 1 della LRTV, considera anche il fenomeno del discorso di odio.

La CETT segue il principio dello Stato emittente, ossia lo Stato in cui ha sede l'emittente che diffonde deve garantire che a questa siano applicate le relative norme. Se un programma estero di uno Stato emittente vincolato dalla CETT che può essere captato in Svizzera viola la CETT, la Svizzera non potrebbe impedire di propria iniziativa l'ulteriore ritrasmissione del programma contestato ma dovrebbe rivolgersi alla parte trasmittente (art. 24 cpv. 1 CETT). Solo in caso di manifesta, seria e grave violazione della Convenzione, lo Stato ricevente può sospendere, a titolo provvisorio, la ritrasmissione del servizio di programmi in questione due settimane dopo averlo comunicato allo Stato trasmittente (art. 24 cpv. 2 CETT)[38]. Nel caso di programmi trasmessi da Stati che non hanno sottoscritto la CETT, la Svizzera non è vincolata alle condizioni dell'articolo 24 CETT. L'articolo 52 capoverso 1 lettera b LRTV dà all'UFCOM la possibilità di limitare o vietare la trasmissione di un programma mediante tecniche di telecomunicazione se le disposizioni di diritto internazionale vincolanti per la Svizzera in materia di programmi, pubblicità o sponsorizzazioni sono violate in modo durevole e grave.

4.4.2.2 Legge federale sulla protezione dei minori nei settori dei film e dei videogiochi (LPMFV)

Il 30 settembre 2022 il Consiglio nazionale e il Consiglio degli Stati hanno adottato la legge federale sulla protezione dei minori nei settori dei film e dei videogiochi (LPMFV; FF *2022* 2406). Questa non è ancora in vigore[39].

---

[36] Consiglio svizzero della stampa, Codice dei giornalisti.

[37] Consiglio svizzero della stampa, parere 8/2016 del 2.5.2016 (X. c. «Tribune de Genève»).

[38] Art. 24 cpv. 2 CETT in combinato disposto con l'art. 52 LRTV.

[39] L'ordinanza è stata sottoposta a consultazione il 16 giugno 2023. Legge e ordinanza entreranno in vigore allo stesso momento. Cfr. Protezione dei minori in materia di film e videogiochi (admin.ch).

La nuova legge federale ha lo scopo di proteggere i minori dai contenuti mediatici di film e videogiochi che potrebbero nuocere al loro sviluppo fisico, mentale, psichico, morale o sociale. Si tratta in particolare di rappresentazioni di violenza (tra cui rientrano anche i contenuti di odio), sesso e scene minacciose. In Svizzera tutti i cinema, i venditori al dettaglio (anche online) e i servizi su domanda sono tenuti a indicare l'età minima necessaria e a svolgere controlli dell'età. Saranno responsabilizzati anche i fornitori di servizi di piattaforma per video e videogiochi (ad es. YouTube, Twitch).

La LPMFV persegue principalmente l'obiettivo di proteggere i bambini e i giovani da contenuti per loro dannosi[40]. Sebbene la legge non preveda misure per impedire esplicitamente i discorsi e la propaganda di odio, tramite l'obbligo imposto al fornitore di istituire sistemi di segnalazione esiste almeno la possibilità di arginare la loro diffusione e visibilità.

4.4.2.3 Revisione totale della legge sulla protezione dei dati

La nuova legge sulla protezione dei dati (LPD; RS 235.1), la nuova ordinanza sulla protezione dei dati (OPD; RS 235.11) e la nuova ordinanza sulle certificazioni in materia di protezione dei dati (nOCPD; RS 235.13) sono entrate in vigore il 1° settembre 2023. Con la revisione totale la LPD viene adeguata alle mutate condizioni tecnologiche e sociali.

Ad esempio, le grandi piattaforme Internet e i social network con sede all'estero sono quindi obbligate a designare un rappresentante in Svizzera se trattano dati personali di persone in Svizzera. In questo contesto, il rappresentante deve fungere da interlocutore per l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) e per le persone interessate in Svizzera (art. 14 cpv. 2 nLPD). La disposizione di cui all'articolo 14 della nLDP mira a facilitare il contatto con gli operatori delle piattaforme Internet in modo che le persone interessate possano far valere meglio i loro diritti, come la soppressione di contenuti diffamatori. L'efficacia di questi punti di contatto sarà dimostrata solo una volta trascorso un certo periodo di tempo dalla sua entrata in vigore.

4.4.2.4 Legge sulle telecomunicazioni

La legge sulle telecomunicazioni (LTC; RS 784.10) disciplina la trasmissione di informazioni mediante telecomunicazione, inclusa la trasmissione di programmi radiotelevisivi. Secondo l'articolo 3 lettera b LTC, fornisce un servizio di telecomunicazione chi trasmette mediante telecomunicazione informazioni almeno tra due parti[41].

La LTC definisce gli obblighi dei fornitori di servizi di telecomunicazione (FST), in cui rientrano tra l'altro gli obblighi di sicurezza, riservatezza, informazione, conciliazione e blocco. Per contro la legge sulle telecomunicazioni non prevede misure contro i discorsi di odio.

Tuttavia, l'ordinanza sui domini Internet (ODIn; RS 784.104.2) disciplina la *procedura* secondo cui fedpol può revocare un nome di dominio svizzero se tramite questo viene diffuso materiale di propaganda violenta (art. 13*e* cpv. 5 lett. a^{bis} LMSI, v. sopra cap. 4.4.1.3)[42]. La procedura di revoca ai sensi dell'articolo 13*e* capoverso 5 lettera a^{bis} LMSI è disciplinata dagli articoli 30 e 31 ODIn: il gestore del registro (attualmente SWITCH per il dominio .ch) revoca l'attribuzione di un nome di dominio se un'autorità amministrativa o preposta al perseguimento penale (in questo caso fedpol) lo ordina nell'ambito delle sue competenze.

---

[40] Messaggio dell'11 settembre 2020 concernente la legge federale sulla protezione dei minori nei settori dei film e dei videogiochi, FF **2020** 7187, 7201, 7213 seg.

[41] Gli operatori delle piattaforme di social media ad es. non rientrano generalmente nel campo di applicazione della LTC poiché nella maggior parte dei casi sono solo una delle parti tra cui vengono trasmesse le informazioni.

[42] Tuttavia, la revoca di un nome di dominio avviene solo quale soluzione estrema se tutte le altre misure ipotizzabili sono risultate vane.

5 Conclusione

I discorsi di odio rappresentano una seria sfida per le società democratiche. Questi impediscono alle persone di partecipare ai dibattiti pubblici, negano loro i diritti umani, promuovono la radicalizzazione e preparano il terreno alla violenza. Si tratta quindi di un attacco alla sfera pubblica delle società democratiche, ai loro membri e alle loro istituzioni.

Sebbene la Svizzera non conosca una categoria giuridica a sé stante per i discorsi di odio, sono proprio le disposizioni del codice penale a rispecchiare in gran parte il contenuto della definizione del Consiglio d'Europa sul discorso di odio. Le maggiori sfide attraverso i diversi settori del diritto si presentano nel campo della sua applicazione. In particolare, il drastico aumento dei discorsi di odio online su piattaforme digitali pone serie sfide alla società e alla politica.

Anche se il diritto penale fornisce vari strumenti per assicurare le prove, le relative richieste di assistenza giudiziaria spesso non vengono tuttavia recepite ad esempio dagli Stati Uniti, dove hanno sede gli intermediari più influenti sul pubblico svizzero. Ciò avviene perché comportamenti considerati atti punibili nell'ambito dell'incitamento all'odio secondo il diritto svizzero, spesso sono consentiti secondo il diritto statunitense, che attribuisce un peso particolarmente elevato alla libertà di espressione. Queste lacune si rivelano ancora più problematiche perché i discorsi di odio si verificano sempre più frequentemente online e si diffondono più velocemente e in maniera più ampia rispetto a quelli offline.

L'applicazione di norme contro il discorso di odio è stata finora lasciata principalmente agli intermediari. Tuttavia, il loro approccio si rivela inaffidabile. Inoltre, le loro condizioni generali differiscono notevolmente dalla legge svizzera e gli standard tra le piattaforme sono molto diversi. In aggiunta, il discorso di odio si sposta su quelle piattaforme che non prevedono quasi alcun limite. Di conseguenza, nel complesso, i discorsi di odio, che sono proibiti e possono essere perseguiti penalmente offline, di fatto non lo sono online.

Con il *Digital Services Act* l'UE ha presentato un approccio che intende apportare miglioramenti a queste lacune, imponendo maggiori obblighi di diligenza agli intermediari e sottoponendoli a controlli. Il principio di questo quadro di co-regolamentazione è la consapevolezza che ciò che è illegale e punibile offline deve esserlo anche online. Singoli Paesi, come il Regno Unito, la Francia o la Germania, hanno inoltre leggi nazionali volte a rafforzare l'applicazione del diritto.

In Svizzera il 5 aprile 2023 il Consiglio federale ha incaricato il DATEC (UFCOM) di preparare un progetto di consultazione sulla regolamentazione delle piattaforme di comunicazione. Questo progetto tratterà in particolare anche le sfide derivanti dalla mancata applicazione della legge nel diritto penale e nel diritto civile (v. cap. **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**).

Nell'ambito del diritto civile, il Consiglio federale attribuisce la priorità alla conclusione di accordi di assistenza legale reciproca e di convenzioni che prevedono il recapito postale diretto di documenti in materia civile.

Nell'ambito delle misure preventive di polizia, nel 2019 il Consiglio nazionale e il Consiglio degli Stati hanno accolto la mozione "Scambio di dati di polizia su scala nazionale" (Mo. 18.3592), in base alla quale le autorità di polizia cantonali devono avere la possibilità di scambiarsi sistematicamente informazioni di polizia tra di loro e con gli organi di polizia della Confederazione. L'attuazione è ora affidata al Consiglio federale. Con il progetto POLAP (piattaforma di ricerca della polizia), la Confederazione e i Cantoni stanno lavorando per migliorare lo scambio nazionale e internazionale dei dati di polizia.

Infine il 30 settembre 2022 il Consiglio nazionale e il Consiglio degli Stati hanno adottato la legge federale sulla protezione dei minori nei settori dei film e dei videogiochi (LPMFV; FF *2022* 2406). Questa prevede l'obbligo di istituire sistemi di segnalazione che dovrebbero contribuire a frenare la diffusione e la visibilità dei discorsi di odio.

Il Consiglio federale non vede quindi al momento alcuna necessità di adottare misure supplementari oltre a quelle summenzionate.