Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA
DIREZIONE CENTRALE PER LA POLIZIA STRADALE, FERROVIARIA, DELLE COMUNICAZIONI E PER I REPARTI SPECIALI DELLA POLIZIA DI STATO
Servizio Polizia Postale e delle Comunicazioni

N. 300.D/2017/784-MS.R/1 Roma, *data del protocollo*

OGGETTO: Relazione alla Commissione straordinaria per il contrasto dei fenomeni di intolleranza, razzismo, antisemitismo e istigazione all'odio e alla violenza del Direttore del Servizio Polizia Postale e delle Comunicazioni, Dott. Ivano Gabrielli, nell'ambito dell'indagine conoscitiva sui discorsi d'odio.

ALLA COMMISSIONE STRAORDINARIA "PER IL CONTRASTO DEI FENOMENI DI INTOLLERANZA, RAZZISMO, ANTISEMITISMO E ISTIGAZIONE ALL'ODIO E ALLA VIOLENZA" DEL SENATO DELLA REPUBBLICA ITALIANA
commissione.antidiscriminazioni@senato.it
ROMA

La Polizia Postale e delle Comunicazioni è un reparto specialistico della Polizia di Stato che opera in prima linea nella prevenzione e nel contrasto della criminalità informatica, a garanzia dei valori costituzionali della segretezza della corrispondenza e della libertà di ogni forma di comunicazione.

Il Servizio Centrale, vertice della struttura, è punto di riferimento nel coordinamento, nella programmazione e nella pianificazione operativa degli uffici periferici della Specialità.

L'attività di prevenzione e contrasto viene supportata da un sistematico coinvolgimento degli organismi di cooperazione internazionale giudiziaria e di polizia, attraverso la condivisione di strategie di monitoraggio e contrasto dei fenomeni concernenti il *cybercrime*.

La Polizia Postale e delle Comunicazioni ha competenze estremamente ampie, alcune delle quali sono esclusive: in particolar modo, forte e puntuale è l'impegno nella prevenzione e nel contrasto degli attacchi cibernetici alle infrastrutture critiche, attraverso l'operatività del **Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche - CNAIPC**, nella lotta alla

pedopornografia *online* e a tutte le forme di aggressione dei minori in rete attraverso l'operatività del **Centro Nazionale per il contrasto alla pedopornografia online - CNCPO**, nella prevenzione del *cyberterrorismo*, nel contrasto dell' *hacking* e del *financial cybercrime*, la repressione dei reati commessi sui *social network*, nonché il contrasto ai reati postali. Ai due Centri si affianca un avamposto virtuale costituito dal **Commissariato di PS online**, portale istituzionale costantemente aggiornato che consente ai cittadini di segnalare, informarsi, chiedere e ottenere informazioni relative alle emergenze *online*.

Nella moderna società, la diffusione della cultura digitale e lo sviluppo dei *social media* offrono al pubblico l'opportunità di essere produttori attivi di contenuti da condividere in rete.

I messaggi veicolati, tuttavia, assumono talora connotazioni offensive e violente dirette verso singoli o verso gruppi, con la finalità di diffondere odio nei confronti di categorie ben definite in base all'etnia, all'orientamento sessuale, alla professione religiosa, alla disabilità o ad altri aspetti.

Relativamente a tali fenomenologie di comportamenti, generalmente identificati con il termine "*hate speech*", non si rinviene, a livello internazionale, una definizione univoca.

Secondo la **Raccomandazione del Comitato dei Ministri del Consiglio d'Europa n. 20, datata 30 ottobre 1997**: «*Il termine -discorso d'odio- o hate speech, deve essere inteso come comprensivo di tutte le forme di espressione che diffondono, incitano, promuovono o giustificano l'odio razziale, la xenofobia, l'antisemitismo o altre forme di odio basate sull'intolleranza, tra cui: intolleranza espressa da nazionalismo aggressivo ed etnocentrismo, discriminazione e l'ostilità contro le minoranze, i migranti e le persone di origine immigrata*».

Per affrontare il tema dell'*hate speech* e, più in generale, di una grossa parte dei fenomeni delittuosi che avvengono sul *web*, non si può prescindere da una premessa iniziale. La rivoluzione digitale degli ultimi quindici anni non è stata soltanto una rivoluzione tecnologica e culturale: siamo di fronte a una vera e propria "rivoluzione antropologica" che caratterizza fortemente e connota tutti i nostri comportamenti. Il nostro vivere quotidiano è tecnomediato dalla rete, che ha assunto un ruolo sempre più importante all'interno della nostra vita per la facilità e la rapidità con cui è possibile compiere azioni reali via *web*, ed è spesso

difficile comprendere il carattere permanente, incisivo e determinante delle azioni "virtuali" che vengono compiute.

Ciò avviene perché lo schermo del computer o il display dello *smartphone*, che si frappongono fisicamente e psicologicamente tra noi e l'oggetto delle azioni virtuali, creano una distanza che ci impedisce di percepire appieno gli effetti e le emozioni generate dalle nostre parole e dai nostri comportamenti, con una conseguente riduzione dei freni inibitori e una sottovalutazione della portata delle nostre azioni, dei pericoli in cui possiamo incorrere nella rete e degli effetti dannosi provocati nell'interlocutore.

Va aggiunto che se da un lato l'aggressività, la rabbia, la violenza sono emozioni e reazioni proprie della natura umana, l'avvento della tecnologia ha profondamente modificato gli effetti e la portata dei reati di odio, che in passato si mantenevano circoscritti all'interno di determinati contesti spazio-temporali, mentre oggi, tramite la rete, possono raggiungere le vittime in ogni luogo ed in ogni momento con una rapidità e pervasività in passato inimmaginabili.

Ciò avviene per diversi fattori. Da un lato, la rete viene spesso percepita come un luogo senza regole nel quale i limiti, come il rispetto dell'altro possono essere valicati senza scrupoli e senza conseguenze. Dall'altro lato, l'assenza fisica di un interlocutore e l'impossibilità di percepire direttamente le sue reazioni, espressioni, il suo linguaggio corporeo (indizi importanti per poter interagire in maniera efficace e orientare tempestivamente il nostro comportamento) determina la mancanza dell'effetto "regolatore" offerto da questi *feedback*.

Si aggiunge a tutto questo l'effetto amplificatorio della presenza di un pubblico potenzialmente vastissimo, un pubblico che può, altrettanto velocemente esacerbare l'espressione d'odio attraverso condivisioni e *like*, con un'onda aggressiva che travolge spesso le vittime con una forza che può arrivare ad essere decisamente superiore alle intenzioni dell'*hater* "primario".

In questo luogo percepito senza regole e senza limiti trovano terreno fertile fenomeni tra loro molto diversi, come il ***body shaming***, tramite insulti e allusioni riferiti a particolari del corpo di una persona, che divengono oggetto di giudizi e valutazioni sui *social network*, allo scopo di mettere in evidente imbarazzo la vittima, o la diffusione non autorizzata sul *web* di filmati e immagini sessualmente esplicite, originariamente destinate a restare private. Tale reato è

stato compiutamente normato con l'entrata in vigore del cd. "Codice rosso"[1] per sanzionare condotte altamente lesive nei confronti delle vittime.

O il *deep fake porn* (o *deepnude*), l'evoluzione di ciò che è stato anni fa lo stupro virtuale[2]. Per *deep fake* si intendono *foto, video e audio* generati mediante l'intelligenza artificiale (AI): partendo da contenuti reali (immagini, video e audio), si riescono a modificare o ricreare, in modo estremamente realistico, le caratteristiche e i movimenti di un volto o di un corpo e a imitare fedelmente una determinata voce. Una particolare forma di *deepfake* è il *deepnude* che consiste nella creazione di contenuti multimediali che ritraggono ignare persone, senza abiti, in situazioni compromettenti o addirittura in contesti pornografici. Particolare allarme desta l'utilizzo di tale tecnologia per generare contenuti pedopornografici attraverso l'apposizione di volti di minori su corpi nudi. Il *deepnude* viene anche utilizzato nella commissione dei reati di *revenge porn* o nel *sexting*. Inizialmente il fenomeno ha coinvolto personaggi famosi allo scopo di screditarli o ricattarli, ma negli ultimi tempi sono stati oggetto di *deepfake* anche persone comuni.

I contenuti generati attraverso l'intelligenza artificiale vengono anche utilizzati per compiere atti di cyberbullismo o per alimentare campagne di disinformazione anche in occasione delle consultazioni elettorali allo scopo di influenzare l'opinione pubblica.

In generale, *l'hate speech online* può essere riconducibile a casistiche molto diverse tra loro, come:

- l'azione di gruppi organizzati, più o meno politicizzati, di stampo discriminatorio, razzista o sessista;
- attacchi di persone singole e/o gruppi informali che colpiscono obiettivi personali. Questo tipo di dinamiche si traducono spesso in **reati di diffamazione, molestie, minacce e *stalking*** che trovano in rete il modo di

[1] "Codice Rosso": 15 casi nel 2022, 31 casi nel 2023, 23 casi dal 1 gennaio all'11 aprile 2024.

[2] Fenomeno che si realizza in gruppi *social* chiusi, dove per soddisfazione narcisistica, per misoginia, divertimento, ragazzi e adulti diffondono immagini private tratte dai profili *social* di ignare donne, incitando allo sproloquio sessuale volgare tutti i frequentatori del gruppo "virtuale", associando ad ogni video e ad ogni immagine, illegalmente condivisa, generalità come nome, cognome e numero di telefono della vittima

aggravarsi e amplificarsi con evidenti enormi e duraturi danni per le vittime;

- giovani e giovanissimi che bersagliano coetanei con insulti, minacce o altri tipi di condotte *online*, secondo dinamiche proprie del **cyberbullismo**;
- singoli o gruppi che in modo ludico-provocatorio colpiscono persone, gruppi o luoghi virtuali al solo scopo di creare dissenso e scompiglio (*troll*). Il termine deriva dal mitologico *troll*, creatura umanoide diffusa, secondo la leggenda, nell'Europa settentrionale, in particolare in Norvegia. Con questo termine si definisce una serie di comportamenti posti in essere da utenti della rete *internet* allo scopo di provocare forti reazioni, messaggi offensivi, scompiglio e litigi sul *web*. I servizi della rete generalmente interessati dal fenomeno sono i *social network*, le *chat*, i forum e tutti quegli spazi *web* nei quali la comunicazione tra gli utenti è l'elemento preponderante. Le tecniche utilizzate e i comportamenti tenuti allo scopo di realizzare "guerre" di insulti consistono spesso nel proporre argomentazioni e tesi diametralmente opposte, incongruenti o insostenibili all'interno di forum tematici. Non è inusuale inoltre che vengano creati gruppi di utenti o pagine di *social network* che inneggiano a comportamenti moralmente, eticamente o giuridicamente inaccettabili;
- esistono anche applicativi di intelligenza artificiale, denominati *Social-Bot*, creati per un utilizzo manipolativo e programmati per ritrasmette e far circolare il più possibile sulla rete *fake news* e messaggi d'odio.

In Italia, l'art. 604 bis del codice penale, nell'ambito dei c.d. delitti contro l'eguaglianza, punisce la propaganda di idee fondate sulla superiorità o sull'odio razziale ed etnico, nonché la commissione o l'istigazione a commettere atti di discriminazione per motivi razziali, etnici, nazionali o religiosi. Tale specifica previsione risulta integrata, in assenza di una fattispecie di reato che fornisca una definizione normativa omnicomprensiva di *hate speech*, con ipotesi delittuose quali la diffamazione aggravata dall'uso di *internet*, le minacce, gli atti persecutori[3].

[3] Art. 604 ter: Circostanza aggravante. Per i reati punibili con pena diversa da quella dell'ergastolo commessi per finalità di discriminazione o di odio etnico, nazionale, razziale o religioso, ovvero al fine di

Il fenomeno in esame, si differenzia sostanzialmente nella sua espressione *on line*, da quella *off line*, per quattro elementi distintivi:

- *il carattere permanente*: il discorso d'odio *on line* tende a rimanere accessibile per lungo tempo, amplificando e prolungando gli effetti dannosi in un periodo temporale di rilevante ampiezza;
- *la caratteristica di contenuti itineranti e ricorrenti*: le espressioni di odio, anche se rimosse, possono riapparire altrove, ad opera di altri utenti sulla stessa o diverse piattaforme;
- *l'associazione all'idea di anonimato e impunità,* che aumenta la propensione degli autori a manifestazioni di odio che difficilmente si esprimerebbero in maniera analoga nella vita reale;
- *la diffusione transnazionale dei contenuti*, alla quale consegue un maggiore impatto sociale rispetto ai contenuti *off line* (un aspetto, quello della transnazionalità, che, quale connotazione tipica delle fenomenologie afferenti al crimine informatico, sottende l'esigenza, anche per *l'hate speech*, di un approccio su base internazionale, ai fini della maggiore efficacia delle strategie di prevenzione e contrasto).

Le categorie colpite sono spesso bersaglio di odiatori seriali, in cerca di un obiettivo su cui riversare la propria rabbia per lenire il proprio senso di frustrazione, altre volte "obiettivi determinati" di meccanismi più complessi e strutturati.

Per affrontare un fenomeno così ricco di sfaccettature e complesso non è detto che il diritto penale (che si pone come *extrema ratio* di attacco ai fenomeni) possa essere di per sé l'unico e ineluttabile strumento di contrasto.

Nell'ambito del contesto operativo, funzionale alla prevenzione ed al contrasto, la Polizia Postale ha da tempo avviato, sull'intero territorio nazionale, strategie operative tese sia all'individuazione delle piattaforme *web* utilizzate per la

---

agevolare l'attività di organizzazioni, associazioni, movimenti o gruppi che hanno tra i loro scopi le medesime finalità la pena è aumentata fino alla metà.
Le circostanze attenuanti, diverse da quella prevista dall'articolo 98, concorrenti con l'aggravante di cui al primo comma, non possono essere ritenute equivalenti o prevalenti rispetto a questa e le diminuzioni di pena si operano sulla quantità di pena risultante dall'aumento conseguente alla predetta aggravante.

veicolazione di tali condotte, al fine di attivare percorsi di collaborazione, sia alla conseguente attività di contrasto mediante identificazione dei soggetti.

In tale direzione viene assicurato un attento e continuo monitoraggio della rete, realizzato 24 ore su 24, dagli operatori della Specialità (anche attraverso l'approfondimento delle segnalazioni effettuate dagli utenti per mezzo del Commissariato di P.S. *on line*) allo scopo anche di intercettare tutti quei comportamenti che violino le norme penali vigenti e che, per la loro "procedibilità d'ufficio", consentano di dare notizia all'A.G. per l'esercizio dell'azione penale.

La Polizia Postale e delle Comunicazioni approfondisce, a livello investigativo, le segnalazioni provenienti dall'UNAR (Ufficio Nazionale Anti discriminazioni Razziali), organismo della Presidenza del Consiglio dei Ministri e dall'OSCAD (Osservatorio per la Sicurezza contro gli Atti Discriminatori), organismo incardinato nel Ministero dell'Interno - Dipartimento della Pubblica Sicurezza.

La costante presenza attiva nel web, assicurata sia a livello centrale sia a livello periferico (attraverso le articolazioni territoriali della Specialità), si concentra, per evidenti ragioni, sui contenuti aperti (pubblicamente accessibili), gli unici visualizzabili allorché si operi in termini di prevenzione.

Giova evidenziare come la chiusura effettuata dai "tradizionali" *social network* (*Facebook* ed *Instagram* su tutti) di centinaia di pagine di account riconducibili anche ad alcuni gruppi italiani, ritenuti dai responsabili delle citate piattaforme "organizzazioni pericolose" che "incitano all'odio" e "promuovono azioni violente"[4], abbia determinato il consistente trasferimento di questi profili su piattaforme di comunicazione meno note.

L'esperienza operativa dell'ultimo periodo, infatti, ha consentito di riscontrare un notevole incremento dei *trend* e delle discussioni all'interno di piattaforme che per la propria *policy* garantiscono l'anonimato, rendendo più complicata l'identificazione degli autori dei messaggi, come *Vk.com* (*Vkontakte*) e *Telegram*.

[4] A livello europeo, un importante passo avanti nell'ottica del contenimento di tale fenomeno delittuoso, e stato realizzato attraverso il "Codice di condotta per lottare contro le forme illegali di incitamento all'odio on line", sottoscritto nel maggio 2016, che definisce il discorso d'odio richiamando la predetta decisione quadro 2008/913/GAI. La sottoscrizione da parte della Commissione europea e di Facebook, Microsoft, Twitter e Youtube impegna, infatti, le predette società a dare una pronta ed efficace risposta nei confronti dei contenuti di incitamento all'odio razziale e xenofobo che vengono segnalati dagli utenti delle citate piattaforme.

Proprio quest'ultima piattaforma, con un crescendo di popolarità, risulta ad oggi tra le preferite per la diffusione di materiale multimediale e soprattutto di comunicazioni riservate, in quanto garantisce un elevato livello di sicurezza dei contenuti condivisi dagli utenti, che possono rimanere anonimi e creare canali con un numero di utilizzatori praticamente illimitato.

La tutela della *privacy* dell'utente costituisce, per il titolare del servizio offerto, una vera e propria "*missione aziendale*", al punto che nell'ambito del "*Telegram Privacy Policy*" viene espressamente dichiarato che le "*informazioni sugli indirizzi I.P. degli utenti potrebbero essere fornite alle Autorità Giudiziarie solo per reati di terrorismo*", escludendo, di fatto, la possibilità di acquisire, agevolmente, utili evidenze investigative, direttamente dalla *Telegram L.L.C.*, allorché si proceda per i reati in esame.

A ciò si aggiunga, per quanto attiene al profilo repressivo, che le attività investigative risultano piuttosto complesse, poiché la maggior parte dei *social network*, o dei molteplici spazi virtuali che ospitano la particolare fenomenologia delittuosa, hanno le proprie sedi sociali all'estero, circostanza che non rende sempre agevole gli approfondimenti investigativi, sovente subordinati all'istruzione, da parte dell'Autorità Giudiziaria, di una richiesta di mutua assistenza legale reciproca (MLAT).

Si riporta, di seguito, una tabella dei casi di *hate speech* e diffamazione *online* trattati nell'anno 2023 e nel periodo di tempo compreso tra il 1 gennaio e l'11 aprile 2024.

CASI TRATTATI	HATE SPEECH	DIFFAMAZIONE ON LINE	TOTALE CASI TRATTATI
Anno 2023	68	2.046	**2.114**
Anno 2024 (dal 1 gennaio all'11 aprile 2024)[5]	32	566	**598**

[5] dati rilevati il 12 aprile 2024 (fonte mattinale 2024).

Alla fine di febbraio 2024, è stata condotta un'operazione che ha portato all'esecuzione di due ordinanze di custodia cautelare a carico di due persone che si sono rese responsabili di ***stalking*** nei confronti di una vittima che sui social aveva esternato la propria esperienza nel delicato percorso di cambio di sesso.

La persona offesa aveva infatti denunciato, in diverse occasioni, agli operatori della Polizia Postale del Centro Operativo per la Sicurezza Cibernetica (COSC) Piemonte-Valle d'Aosta, di essere vittima di ripetute offese, minacce e pubblicazioni di dati personali su diversi canali attivati presso una nota piattaforma di *streaming*, mediante registrazioni e dirette in cui veniva in particolare attaccata con manifestazioni di odio transfobico, con l'obiettivo di indurla ad interrompere il proprio iter di transizione di genere o comunque di farla tacere circa la propria condizione emotiva.

All'*hate speech* erano seguiti anche episodi di pedinamento fisico ai suoi danni, diffusione dei dati anagrafici, ricatti rivolti alla vittima in privato sui profili social, rinforzati anche dalla prospettazione del particolare ruolo lavorativo dell'interlocutore, che si spacciava quale "*funzionario del Ministero dell'Interno*", in grado di conoscere in ogni momento spostamenti e dettagli della vita personale del proprio "*target*", fino ad arrivare a minacce di morte.

Erano stati anche creati numerosi *account* collegati a siti erotici o di incontro, contenenti alcuni dati personali della vittima che avevano, al pari, contribuito a ingenerare nella stessa ansie e timori di rimanere vittima di altri attacchi virtuali, o peggio di aggressioni fisiche ad opera di malintenzionati che potessero facilmente rintracciarla nell'ambiente urbano.

Gli accertamenti svolti dalla Polizia Postale, sotto la direzione della Procura di Torino, hanno consentito di incrociare una serie di tracce informatiche e dati di interesse investigativo, consentendo di risalire ai due indagati: in particolare, uno dei due era autore delle dirette *streaming* di carattere denigratorio; l'altro, in possesso di credenziali di accesso a banche dati contenenti dati personali in ragione della propria attività lavorativa, era riuscito a carpire illecitamente i dati

anagrafici successivamente diffusi, motivo per cui si ipotizza nei suoi confronti anche il delitto di accesso abusivo a sistema informatico o telematico[6].

Molti casi di *hate speech* trattati dalla Polizia Postale, sulla base di denunce sporte da singole persone, associazioni e gruppi informali, hanno integrato fattispecie delittuose più gravi.

Per i reati di diffamazione, atti xenofobi, razzisti e di discriminazione di genere, a fronte dei 2.712 casi trattati[7], nel 2023 sono state indagate 535 persone e, tra il 1 gennaio e l'11 aprile 2024, sono state indagate 220 persone per le medesime fattispecie delittuose.

Per quanto concerne, invece, i casi in cui le espressioni d'odio hanno contribuito a integrare il reato di ***revenge porn,*** la Polizia Postale, a fronte dei 368 casi[8] trattati, ha indagato nel 2023 115 persone e, dal 1 gennaio all'11 aprile 2024, 25 persone per le medesime fattispecie delittuose.

Molte sono le iniziative legislative messe in campo per contrastare il fenomeno dell'*hate speech.*

In ambito europeo, in accordo con quanto stabilito dalla decisione quadro 2008/913/GAI del Consiglio, sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale, già con l'Agenda europea sulla sicurezza del 2015, è stato istituito, su iniziativa della Commissione, un Internet Forum, che riunisce i Ministri degli Interni degli Stati membri dell'Unione Europea, nonché i rappresentanti dei principali fornitori di servizi via Internet, del Parlamento europeo, di Europol e il coordinatore europeo per la lotta al terrorismo. Obiettivo del Forum è quello di individuare sistemi che ostacolino la diffusione di contenuti che inneggiano all'odio, alla violenza e al terrorismo internazionale. In esito a siffatta iniziativa, è stata predisposta un'attività di rilevazione e monitoraggio della casistica del fenomeno, al fine di creare sempre maggiore consapevolezza nei cittadini e nelle istituzioni, a cui si è affiancata la previsione di iniziative di *counter-speech*, con l'obiettivo, da un lato, di spiegare il

[6] Sono ancora in corso ulteriori accertamenti volti ad approfondire nel dettaglio le dinamiche sottese alla vicenda e i due indagati devono essere ritenuti non colpevoli fino a sentenza definitiva.
[7] Dal 1 gennaio 2023 all'11 aprile 2024.
[8] Dal 1 gennaio 2023 all'11 aprile 2024.

perché l'odio sia profondamente anti-democratico, dall'altro, di riaffermare i valori che lo stesso mette in pericolo.

All'approccio statistico-culturale si è accompagnata, poi, la sollecitazione delle piattaforme web a porre in essere meccanismi di prevenzione e rimozione dei contenuti offensivi pubblicati sui loro portali. Sotto questo profilo, particolarmente significativo risulta l'accordo raggiunto tra la Commissione Ue e i principali intermediari di servizi internet (*Microsoft, Facebook, Twitter e Youtube*; successivamente, *Instagram, Google+, Snapchat e Dailymotion*), con cui è stato elaborato un codice di condotta finalizzato a contrastare le condotte di *hate speech*.

Tra i numerosi impegni assunti, si possono indicativamente citare l'adozione di procedure chiare ed efficaci per esaminare le segnalazioni riguardanti forme illegali di incitamento all'odio nei servizi da loro offerti, in modo da poter rimuovere tali contenuti o disabilitarne l'accesso; l'adozione di linee-guida indirizzate alla comunità degli utenti della rete, che precisino il divieto di ogni forma di istigazione all'odio e alla violenza; l'obbligo di esaminare, entro 24 ore dalla ricezione, la maggior parte delle segnalazioni (valide) di illecita istigazione all'odio nei servizi offerti dal provider e, se necessaria, la rimozione di tali contenuti o la disabilitazione dell'accesso al sito.

Con riferimento al contesto operativo concernente il fenomeno dell'*hate speech*, la Polizia Postale e delle Comunicazioni, oltre all'attività di contrasto, pone in atto un'intensa e costante opera di prevenzione nei confronti dei descritti fenomeni, soprattutto quando interessano le fasce più vulnerabili della popolazione, quale quella dei minori.

L'impegno in chiave preventiva si esplica, da anni, mediante la realizzazione di campagne di sensibilizzazione, nazionali e locali, allo scopo di responsabilizzare, soprattutto le giovani generazioni, sulle conseguenze dell'uso di un certo tipo di linguaggio in *rete* e nelle relazioni personali: l'obiettivo è quello di guidare i nativi digitali ad avere un rapporto equilibrato con i dispositivi che utilizzano, nella convinzione che all'incremento dei fenomeni legati, in generale, a qualsiasi comportamento lesivo della dignità umana si debba contrapporre la promozione della cultura del dialogo per favorire l'inclusione, la tolleranza e la comprensione "dell'altro".

Tra le iniziative più significative, la campagna itinerante denominata "Una vita da Social", realizzata in collaborazione con il Ministero dell'Istruzione e del

Merito nell'ambito del progetto "Generazioni Connesse", che nel giugno 2023 ha anche travalicato i confini nazionali, raggiungendo alcune città albanesi. L'iniziativa, giunta oramai alla sua 11^ edizione, è ripresa a pieno ritmo con l'inizio dell'anno scolastico 2023-2024. A bordo dell'iconico *truck* simbolo dell'iniziativa, che si trasforma in una vera e propria aula multimediale, vengono accolte dagli operatori della Specialità numerose scolaresche e cittadini, a cui vengono illustrate tutte le più attuali insidie della rete e forniti utili strumenti per un corretto utilizzo del *web*. L'impegno profuso in tale ambito ha consentito, nel corso dell'anno, di realizzare incontri con 2.300 istituti scolastici e di veicolare contenuti educativi a oltre 335.000 studenti, 22.936 docenti e 17.385 genitori.

Accanto a "*Una vita da Social*", merita menzione il progetto *#cuoriconnessi*, una campagna educativa, realizzata in collaborazione con Unieuro, incentrata sul tema del cyberbullismo. Il 6 febbraio scorso, in occasione del *Safer Internet Day*, giornata mondiale per la sicurezza in Rete, all'interno dei *Lumina Studios* di Roma, si è svolto l'evento di presentazione di *#cuoriconnessi*. L'iniziativa, giunta all'ottava edizione e nata nel 2016 per sensibilizzare i giovani, i loro genitori e gli insegnanti sull'uso consapevole della Rete e per prevenire i fenomeni del bullismo e del cyberbullismo, è stata seguita in diretta streaming da oltre 225.000 ragazzi delle scuole di tutta Italia.

In occasione degli incontri, infatti, particolare attenzione viene rivolta principalmente all'allarmante fenomeno del cyber-bullismo, molto diffuso tra i giovani, che come noto, ha trovato una definizione normativa, nella ***Legge n. 71/2017*** secondo cui per *cyberbullismo* si intende "*qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo*".

Le condotte che integrano la definizione di *cyberbullismo* altro non sono che atti di intimidazione, sopraffazione, oppressione fisica e psicologica, commessi in modo intenzionale e ripetuto nel tempo, che si consumano in rete, tramite i social, sulle chat di messaggistica. Tutti questi comportamenti, che si risolvono in aggressioni, molestie, ricatti, ingiurie, denigrazioni, diffamazioni ovvero furti d'identità, alterazioni, manipolazioni, acquisizione o trattamento illecito di dati

personali, realizzati per via telematica, integrano ipotesi di reato previste dall'ordinamento.

Spesso più soggetti si coalizzano contro la vittima prescelta. Molti episodi di *cyberbullismo* nascono da reali ostilità personali, prese in giro tra compagni di scuola, che alimentano forme di aggressione amplificate dalla rete e dalle sue possibilità di "contagio", con gravi ripercussioni psicologiche sulla vittima.

La ***Legge n. 71/2017*** ha introdotto tra le nuove forme di tutela la possibilità di inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete Internet. Se non si provvede entro 48 ore, l'interessato può rivolgersi al Garante della Privacy che interviene direttamente entro le successive 48 ore.

In caso di episodi di bullismo via web, il Questore può ammonire l'autore con un provvedimento analogo a quello adottato per lo ***stalking***: fino a quando non sia stata presentata querela o denuncia per i reati di ingiuria, diffamazione, minaccia o trattamento illecito di dati personali commessi, mediante Internet, da minorenni sopra i 14 anni nei confronti di altro minorenne, il questore potrà convocare il minore responsabile (insieme ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale), ammonendolo oralmente ed invitandolo a tenere una condotta conforme alla legge.

La tabella che segue descrive i casi trattati nell'anno 2023, suddivisi per età delle vittime e raffrontati con gli analoghi dati degli anni precedenti.

CYBERBULLISMO	TOTALE casi trattati	Casi trattati vittime 0-9 anni anni	Casi trattati vittime 10-13 anni	Casi trattati Vittime 14-17 anni
Anno 2023	291	8	72	211
Anno 2024 (DAL 01.01 AL 11.04.2024) [9]	103	6	31	66

[9] Dati rilevati il 12 aprile 2024; fonte mattinale 2024.

La prevenzione e la sensibilizzazione rappresentano per la Polizia Postale e delle Comunicazioni la modalità elettiva per affrontare questo genere di problematiche e per promuovere una tutela che sia sempre più efficace e partecipativa: da anni ingenti risorse umane, specializzate e formate sui temi dell'approccio ai giovani e sui correlati psicologici dell'uso delle nuove tecnologie, vengono impegnate quotidianamente in incontri scolastici con i ragazzi, nella conduzione di seminari e meeting anche online, in cui gli studenti possano ascoltare da operatori di polizia consigli su come proteggersi e suggerimenti finalizzati ad una responsabilizzazione delle proprie azioni in rete e ad un uso consapevole del web.

Focus sulla situazione medio-orientale in relazione alle possibili conseguenze sui fenomeni di discorso d'odio on line e disinformazione.

Con riferimento all'attuale contesto geopolitico in Medio Oriente, si può osservare che gli ultimi avvenimenti occorsi in quell'area geografica hanno determinato, sin dai primi momenti, fenomeni inerenti la diffusione di disinformazione e la condivisione di contenuti multimediali spesso connotati dal tenore antisemita e xenofobo-razziale.

Contestualmente agli attacchi terroristici di *Hamas* e alla risposta di Israele con "*Operation Iron Swords*", è stato registrato un particolare fermento da parte di diversi *account* sui social, responsabili della diffusione di disinformazione e condivisione di video falsi e fuori contesto.

I contenuti sono stati veicolati da diversi account sulle principali piattaforme di comunicazione, nonché sui principali social, tra i quali *X* (*ex twitter*), particolarmente attivi e fregiati della spunta blu di verifica, con l'obiettivo di supportare narrative a sostegno di una o dell'altra fazione, alimentando un caos informativo che contribuisse a confondere la realtà dei fatti. Significativo anche l'intervento della propaganda filorussa, che sta sfruttando la situazione per distogliere l'attenzione dal conflitto ucraino e accusare l'Occidente di essere poco interessato alle questioni mediorientali.

La situazione è esacerbata dal nuovo *business model* di *Twitter* che prevede un *boost* per i post condivisi da account che hanno acquistato sottoscrizioni premium e per questo motivo "verificati". Infatti, si è potuto osservare come quasi sempre

la diffusione di video falsi e fuori contesto sia stata portata avanti proprio da *account* con la spunta blu, mentre le voci sul campo, che un tempo rendevano *Twitter* una piattaforma utile per seguire conflitti in fase di sviluppo, vengono soppresse o messe in secondo piano.

Utenti verificati su *Twitter* hanno condiviso presunti video di attacchi su *Gaza* da parte dell'esercito israeliano e offensive di *Hamas* contro gli obiettivi nemici: da un'analisi più approfondita e attenta, invero, risulta che questi contenuti sono riconducibili a eventi passati ma sono stati riproposti, in maniera strumentale, come se fossero riferibili ad attacchi attuali.

Molti account specializzati in materia *OSINT* e agenzie autorevoli hanno dimostrato in più di un'occasione la falsità di tali video. Il rischio intrinseco di questo tipo di attività di disinformazione è quello di utilizzare materiale audiovisivo, estrapolato dal suo contesto originario, a supporto di narrative particolari a favore di una o dell'altra fazione, contribuendo a confondere la realtà dei fatti.

Al riguardo, l'U.E. ha inviato una lettera al patron di *X*, *Elon Musk*, diffidandolo dal diffondere contenuti illegali e disinformazione attraverso la sua piattaforma.

La lettera è stata firmata dal Commissario al Mercato Unico *Thierry Breton* che ha chiesto a *Musk* di contattare entro 24 ore le competenti autorità per rispondere alle contestazioni che gli sono state mosse. Nella lettera *Breton* scrive a *Musk* che "*dopo gli attacchi terroristici condotti da Hamas contro Israele*" a Bruxelles si dispone "*di dare indicazioni sull'utilizzo della sua piattaforma per la diffusione di contenuti illegali e di disinformazione nell'Ue*". La Commissione Europea ha contestato in particolar modo che *X* non abbia agito tempestivamente a fronte di segnalazioni su contenuti illegali, come previsto dal *Digital Service Act* per i gestori di piattaforme social. La richiesta di *Breton* è legata alle immagini estremamente violente sulle azioni dei terroristi, diffuse attraverso il *social network* con l'obiettivo di aumentare l'insicurezza degli israeliani, secondo la lettera.

Il proprietario di *X* ha risposto a tale ultimatum dell'U.E. affermando che la loro politica è quella di essere completamente trasparenti, applicando alcuni aggiornamenti delle proprie *policy*, rimuovendo le precedenti restrizioni relative alla diffusione di contenuti "difficili", credendo che "sia nell'interesse del pubblico comprendere ciò che sta accadendo in tempo reale", come spiegato dal team di sicurezza di X. Allo stesso tempo, ha assicurato al pubblico di lavorare

duramente per bloccare "nuovi account affiliati a Hamas", ai sensi della sua politica sulle entità violente e odiose, menzionando, infine, i suoi continui sforzi congiunti con il Global Internet Forum per contrastare il terrorismo (GIFCT) per prevenire la diffusione di " contenuti terroristici".

A complicare ancora di più la situazione, come già accennato sopra, è l'uso della disinformazione da parte della propaganda filorussa con l'obiettivo di distogliere l'attenzione della Comunità Internazionale dal conflitto russo-ucraino e contribuire a mettere in cattiva luce l'Ucraina.

Infatti, in seguito agli attacchi di Hamas in Israele il 7 ottobre, la Russia ha amplificato diverse operazioni di disinformazione accusando l'Occidente di aver trascurato i conflitti in Medio Oriente. Esempio significativo è la diffusione di report falsi da parte di noti propagandisti russi come Alexander Kots, YevgenyLisitsyn, Ruslan Ostashko, e Yan Gagin.

Questi report hanno sotenuto l'uso di armi ucraine da parte di Hamas per portare avanti le operazioni contro Israele, fatti che sono stati sfatati dal Centro per il Contrasto alla Disinformazione ucraino. In questo contesto, sullo sfondo del conflitto scoppiato in Medio Oriente, diversi canali Telegram filorussi hanno lanciato una campagna di disinformazione per screditare l'Ucraina e l'esercito di Kiev.

Nell'ambito di queste attività malevole, i propagandisti hanno pubblicato un video con modelli di armi occidentali con la didascalia "Hamas ringrazia l'Ucraina per avergli venduto le armi". In un'altra pubblicazione, i propagandisti hanno condiviso notizie false secondo cui i soldati israeliani avrebbero catturato terroristi con armi provenienti dall'Ucraina. Questa non è la prima volta che la Russia conduce tali attività. In precedenza, il Centro aveva riferito della campagna di disinformazione russa sull'uso delle armi ucraine durante le proteste in Francia.

Con specifico riferimento agli aspetti inerenti il contesto nazionale, a seguito del conflitto in Medio Oriente, si osserva che le pubbliche manifestazioni organizzate in segno di solidarietà a sostegno della popolazione palestinese ovvero dello stato israeliano, e quelle non formalmente preavvisate, potrebbero costituire l'occasione per innescare pericolose situazioni di tensione, con il rischio di escalation violente tanto tra gli appartenenti a comunità direttamente

riconducibili al teatro di crisi quanto tra i sostenitori delle stesse, peraltro di frequente attestati su posizioni ideologiche contrapposte.

Al riguardo, nell'ambito dei fenomeni specificatamente neofascisti e neonazisti riconducibili al mondo virtuale, la costante attività di raccolta informativa ha permesso di rilevare come nel corso dell'ultimo periodo risultino ulteriormente incrementate le discussioni all'interno di chat in diverse piattaforme, in particolar modo su *Telegram* e su tutte quelle che per la propria *policy* garantiscono l'anonimato e rendono più complicata l'identificazione degli autori dei messaggi.

Inoltre, dall'inizio del conflitto israelo-palestinese è stato registrato un notevole incremento di segnalazioni riguardanti il fenomeno dell'antisemitismo provenienti sia dall'Osservatorio per la Sicurezza contro gli atti Discriminatori (OSCAD), sia dal Commissariato di PS On Line, ove giungono denunce per reati legati alla xenofobia e all'antisemitismo e istigazione all'odio.

Nello specifico il Servizio Polizia Postale e delle Comunicazioni ha raccolto dall'inizio del conflitto circa 101 segnalazioni dell'OSCAD, nonché più di 95 dal Commissariato di PS online, riguardanti il fenomeno di intolleranza, razzismo, antisemitismo e istigazione all'odio.

In tale contesto il Servizio Polizia Postale e delle Comunicazioni delega i Centri Operativi per la Sicurezza Cibernetica che, di concerto con le locali D.I.G.O.S. svolgono specifiche attività info-investigative sul *web*, al fine di individuare ogni eventuale notizia di minaccia e contrastare il compimento di iniziative che possano turbare l'ordine e la sicurezza pubblica.

IL DIRETTORE DEL SERVIZIO
Gabrielli