RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0051

Internet: quando la "rete" cattura i minori

Domenico Alfieri

La sicurezza in rete dei minori è un tema complesso che coinvolge in cascata le istituzioni di ogni livello. Numerose sono le iniziative volte alla definizione di policy e best practice per tentare di arginare i fenomeni connessi al rapporto, ormai morboso, che i minori hanno con il mondo digitale con il quale entrano in confidenza prima ancora della scolarizzazione. L'educazione digitale va affrontata in modo capillare a partire dal legislatore fino all'educatore, quest'ultimo spesso troppo lento per stare dietro alla frenesia della rete a cui sono sottoposte le nuove generazioni. Questo lavoro riassume sinteticamente alcune delle principali minacce presenti in rete e le loro ripercussioni sulla salute dei minori, offrendo una panoramica su alcune tra le iniziative strategiche intraprese in ambito europeo e nazionale, al fine di sottolineare l'importanza della formazione e della prevenzione ad ogni livello educativo.

Minori – Cyberbullismo – Strategia – Protezione – Abuso

1. Introduzione

Da un progetto finalizzato ad applicazioni militari e strategiche, nacque la prima rete (ARPANET) che consentiva lo scambio di dati tra nodi estremamente distanti dal punto di vista geografico.

Essendo un progetto di ricerca, non ci volle molto che il sistema diventasse un mezzo di scambio di dati e informazioni tra i ricercatori, creando già negli anni Settanta una rete universitaria di ricerca basata su un insieme di regole, chiamate protocolli di rete, che garantissero l'interoperabilità tra le diverse macchine collegate (protocollo TCP/IP).

La semplicità di diffusione, la sua versatilità, l'offerta di contenuti multimediali applicati allo svago, al lavoro e allo studio, favorirono lo sviluppo esponenziale di questo sistema di comunicazione che, negli anni Novanta ebbe un boom vero e proprio trasformandosi in un fenomeno socio culturale senza precedenti che prese il nome di Internet.

Proprio la sua caratteristica di diffusione capillare fece sì che Internet attirasse l'interesse dei privati che attraverso grandi investimenti favorirono l'ampliamento della rete a livello capillare, migliorando qualità e velocità di trasmissione e portandola a diventare quello che oggi è sotto gli occhi di tutti.

Una delle definizioni che viene data a Internet è "La rete delle reti", ma questa rete, che per sua natura tende ad essere sregolata e anarchica, racchiude nella sua definizione due spaccati della realtà diametralmente opposti. Se da un lato infatti si beneficia di uno strumento in cui tutte le maglie sono connesse tra loro consentendo una forma di comunicazione integrata e universale, dall'altro la "rete" è una ve-

D. Alfieri è funzionario informatico del Ministero dello Sviluppo Economico - D.G. per le Tecnologie delle Comunicazioni e la Sicurezza Informatica, Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (DGTCSI-ISCTI). È anche consigliere nel GAC-ICANN per l'Italia.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

ra e propria trappola per chiunque ne sottovaluti la pericolosità facendone un uso inappropriato.

Le minacce presenti nel mondo virtuale sono molteplici e quotidianamente si manifestano con problemi quali:
- il furto d'identità,
- l'esfiltrazione di dati sensibili,
- la violazione della privacy,
- la compromissione di sistemi informatici a volte anche di operatori di servizi essenziali,
- le truffe online,
- i fenomeni di dipendenza,

tutti legati a un suo utilizzo inappropriato o incauto.

Per far fronte a queste minacce nascono degli studi e delle norme sulla sicurezza delle reti e delle informazioni, si formano organismi atti a garantire il rispetto di determinati standard di sicurezza e di determinate regole a tutela delle imprese e del cittadino.

Tutti gli studi e le norme prevedono ovviamente una componente tecnica basata sullo sviluppo e miglioramento a ciclo continuo delle policy di sicurezza e delle tecniche di cybersecurity, e una componente fondamentale che coinvolge il fattore umano. Tale componente può essere definita come una sorta di educazione digitale, ovvero quel processo di formazione imprescindibile alla prevenzione delle minacce informatiche sia a livello d'impresa che a livello domestico/scolastico.

2. Impatto della rete sui minori

I risvolti negativi che caratterizzano la rete si ripercuotono nell'ambiente domestico e scolastico, in particolare nell'utilizzo di Internet da parte dei minori, per cui diventa necessario focalizzare l'attenzione allo sviluppo di un processo educativo orientato alle nuove generazioni.

In termini di apprendimento la rapidità dei "nativi digitali" si contrappone alla lentezza degli adulti che spesso si ritrovano a dover accettare passivamente, e a volte superficialmente, un'evoluzione che non riescono a seguire, spesso a discapito dell'azione protettiva che dovrebbero esercitare.

Con il 69% dei giovani online nel 2019 e un bambino su tre con accesso alla rete da casa, Internet è diventato parte integrante della vita dei minori, offrendo ai bambini e ai giovani molte possibilità di comunicare, imparare, socializzare e giocare, esponendo i bambini a nuove idee e fonti di informazione più diversificate e offrendo loro opportunità di partecipazione politica e civica in modo che crescano, siano creativi e contribuiscano significativamente a una società migliore.

Con i bambini lontani dal loro edificio scolastico e che imparano a distanza, nel 2020 e nel 2021 la pandemia di COVID-19 ha delineato l'importanza di una connettività affidabile come mezzo imprescindibile per l'accesso all'istruzione di base, alle interazioni sociali, e ai servizi di assistenza e supporto.

L'accesso alla connettività è sempre più un fattore determinante delle pari opportunità per i bambini, in particolare per coloro che sono lasciati indietro nei sistemi attuali a causa di povertà, disabilità, etnia, genere, sfollamento o isolamento geografico. L'Information Technology può aiutarli ad esprimere il loro potenziale educativo, facilitare la loro inclusione sociale e amplificare la loro voce nella partecipazione civica, in conformità ai loro diritti sanciti della Convenzione delle Nazioni Unite sui diritti dell'infanzia (UN CRC).

Pur sostenendo e promuovendo i diritti dei bambini, lo stesso ambiente online può esporre i bambini a rischi, alcuni dei quali possono tradursi in potenziali danni.

Infatti l'impalpabilità della rete ha fatto sì che tutto ciò che prima accadeva sotto gli occhi di tutti, per cui facilmente riscontrabile, adesso si sviluppi in modo silente e possa sfuggire al controllo di chi dovrebbe tutelare gli individui più fragili.

Solo nell'aprile 2020, il *National Center for Missing and Exploited Children* - NCMEC ha registrato quattro milioni di segnalazioni di sospetto materiale pedopornografico online, rispetto a un milione registrato nel 2019 nello stesso periodo.

La pandemia di COVID-19 ha dunque aggravato le minacce precedentemente esistenti per i bambini online ed ha sottolineato l'urgente necessità di agire per la prevenzione di rischi quali:
- rischi sui contenuti: esposizione a informazioni imprecise o incomplete, contenuti inappropriati o addirittura criminali come esposizione a contenuti per adulti/estremisti/violenti/crudi, autolesionismo, comportamenti distruttivi e violenti, di radicalizzazione o adesione a contenuti razzisti o discriminatori idee;
- rischi di contatto da parte di adulti o coetanei: molestie, esclusione, discriminazione, diffamazione e danno alla reputazione, abusi e sfruttamento sessuale incluse estorsioni, adescamento (sessuale), materiale pedopornografico, traffico e sfruttamento sessuale dei bambini anche nei viaggi e nel turismo;
- rischi di tipo contrattuale: esposizione a rapporti contrattuali inappropriati, consenso dei minori online, marketing integrato, gioco d'azzardo online nonché violazione e uso improprio di dati per-

sonali come pirateria informatica, frode e furto di identità, truffe, profiling bias;
- rischi comportamentali: come la condivisione di contenuti sessuali autogenerati o rischi caratterizzati da attività dei coetanei: ostilità e violenza come il cyberbullismo, lo stalking, l'esclusione e le molestie.

Dei rischi appena descritti ce ne sono alcuni che si verificano all'ordine del giorno, tra cui:

il cyberbullismo si può definire come la manifestazione in rete di azioni violente e intimidatorie esercitate da un bullo, o un gruppo di bulli, tramite strumenti elettronici nei confronti di un coetaneo incapace di difendersi. Tali azioni che prima riguardavano molestie verbali, aggressioni fisiche e persecuzioni generalmente attuate in ambiente scolastico, adesso si manifestano nelle case delle vittime e in ogni momento della loro vita, perseguitandole con messaggi, immagini, video offensivi inviati tramite smartphone o pubblicati sui siti web tramite Internet.

La pedopornografia (pornografia minorile) è configurabile come ogni rappresentazione, con ogni mezzo, di un minorenne in attività sessuali esplicite, reali o simulate, o qualsivoglia rappresentazione degli organi sessuali per scopi sessuali. Direttamente collegata alla pedopornografia c'è l'adescamento dei minori in rete (*grooming*).

Il *grooming* è una particolare forma di cyberbullismo che sfocia nell'adescamento sessuale. Il predatore si guadagna la fiducia del minore dimostrandosi amico e sviluppando una relazione intima e duratura che può sfociare poi in un incontro sessuale o in uno scambio di materiale pedopornografico.

Tutti fenomeni legati ad un abuso della rete che sfocia nella dipendenza, un fenomeno silente che si verifica con l'abuso degli strumenti informatici da cui scaturisce una mania o una fissazione che a sua volta porta a confondere il piano della vita virtuale con quello della vita reale.

3. Problema trattato a livello internazionale

I problemi da affrontare in ambito di educazione digitale sono molteplici e non potevano non suscitare un interesse a livello globale. Tale interesse ha portato allo sviluppo di leggi, policy, linee guida che hanno stimolato l'interesse della comunità a livello internazionale.

Il tema della protezione online dei minori (*Child Online Protection*) richiede tutt'oggi una risposta globale basata sulla cooperazione internazionale e sul coordinamento nazionale.

Le sfide e le minacce persistono a causa della natura senza confini dell'ambiente online che rende difficili iniziative significative come la formazione di quadri legislativi, piani, strategie, risorse, compresi finanziamenti e istituzioni internazionali e nazionali dedicate a garantire la protezione online dei minori.

Per intraprendere un processo di prevenzione e protezione è necessario adottare a tutti i livelli una strategia inclusiva e multilivello di protezione online dei minori con misure e attività efficaci e mirate, che includono risorse finanziarie e umane. Solo con un approccio multi-stakeholder coordinato e cooperativo i bambini e le generazioni future saranno protetti e autorizzati a prosperare negli ambienti digitali.

In ambito europeo nasce la *European strategy for a better Internet for our children*, che introduce la necessità di contenuti online di qualità nonché l'incremento delle competenze e degli strumenti per utilizzare Internet in modo sicuro e responsabile. Considerata l'età in cui i minori si avvicinano al mondo virtuale, alcuni addirittura prima di saper leggere e scrivere, diventa una necessità lavorare sui contenuti e sulla formazione, stimolando al contempo il potenziale del mercato sui contenuti online interattivi, creativi ed educativi.

La Commissione europea, che segue gli sviluppi della strategia, propone una serie di azioni raggruppate verso i seguenti obiettivi:
- stimolare la produzione di contenuti online creativi ed educativi per i bambini e promuovere esperienze online positive per i più piccoli;
- aumentare la consapevolezza, compresa l'alfabetizzazione digitale e la sicurezza online in tutte le scuole dell'UE;
- creare un ambiente sicuro per i bambini attraverso impostazioni di privacy adeguate all'età, un uso più ampio dei controlli parentali e classificazione in base all'età e ai contenuti;
- lottare contro il materiale pedopornografico online e lo sfruttamento sessuale dei minori.

La strategia coinvolge, oltre la Commissione europea, i paesi dell'UE, gli operatori di telefonia mobile, i produttori di telefoni e i fornitori di servizi di social networking per fornire soluzioni concrete per un Internet migliore per minori.

I compiti svolti dalla Commissione europea in merito alla strategia si sviluppano principalmente attraverso l'attuazione del meccanismo per collegare l'Europa e gli strumenti per il finanziamento dell'infrastruttura dei servizi digitali.

La strategia europea ha influenzato le politiche nazionali nella maggior parte dei paesi dell'UE. Ogni anno, varie azioni e campagne nell'ambito della Stra-

tegia raggiungono migliaia di scuole e giovani, ma anche genitori e insegnanti[1].

Uno degli organismi di rilievo internazionale che si è occupato del tema "tutela dei minori in rete" è l'ITU - *International Telecommunication Union*.

L'ITU ha infatti dedicato alla protezione dei minori in rete una sezione sul proprio sito Internet, all'interno della quale sono presenti linee guida e video lezioni dedicate alla sicurezza in rete dei bambini.

Nella pubblicazione *Keeping children safe in the digital environment: The importance of protection and empowerment*, viene affrontato il problema come *global challenge* (sfida globale) evidenziando come i rapidi progressi della tecnologia, della società e della natura senza confini di Internet richiedano una protezione online dei minori agile e adattiva, pena la sua inefficacia.

La protezione online dei minori necessita di una strategia olistica che favorisca la formazione di ambienti digitali sicuri, rispettosi del genere, adeguati all'età, inclusivi e che sia caratterizzata da:

- un approccio basato sui diritti dell'infanzia, sostenendo i principi sanciti dalla CRC - *Convention on the Rights of the Child* delle Nazioni Unite[2] e dal *General comment No. 25 (2021) on children's rights in relation to the digital environment*[3];
- un equilibrio dinamico tra garanzia di protezione e pari (e sicure) opportunità ai bambini di essere cittadini digitali;
- la prevenzione di eventuali danni;
- una risposta incentrata sul bambino, che sostenga una formazione incentrata sulla responsabilizzazione di fronte alle minacce, con specifico riferimento all'emergenza COVID-19 e agli scenari ad essa connessi.

Questo approccio prevede anche la partecipazione dei minori alla progettazione, implementazione e valutazione delle soluzioni per mantenerli al sicuro nell'ambiente virtuale.

Al fine di rispondere efficacemente ai rischi e ai danni online per i minori diventa necessario adottare una strategia nazionale di protezione inclusiva e multi-stakeholder che integri lo sviluppo di nuove policy con quelle già esistenti fornendo il quadro strategico necessario per affrontare la sfida globale della protezione dei minori in rete.

Tale strategia dovrebbe rafforzare un coordinamento efficace considerando l'importanza, la visione e il ruolo delle seguenti parti interessate:

- governo a livello locale, nazionale e regionale (ad es. affari interni, salute, istruzione, giustizia, assistenza sociale/protezione dell'infanzia, digitale/informazioni, legislatori);
- forze dell'ordine;
- organizzazioni di servizi sociali e sanitari (ad es. consulenza, servizi di supporto, ufficio per il benessere dei giovani, case sicure, riabilitazione, servizi sanitari);
- industria ICT, ad es. piattaforme online, fornitori di contenuti, fornitori di servizi Internet (ISP) e altri fornitori di servizi elettronici (ESP), fornitori di reti di telefonia mobile, fornitori Wi-Fi pubblici;
- organizzazioni internazionali, ONG, OSC e organizzazioni comunitarie (ad esempio, protezione dei minori e altre organizzazioni internazionali e ONG pertinenti, sindacati e organizzazioni di insegnanti/genitori);
- bambini e giovani, nonché i loro genitori/tutori;
- comunità accademica e di ricerca (es. *think tank*, centri di ricerca, biblioteche, scuole e università).

Una strategia nazionale di protezione dei minori online fornisce la tabella di marcia per riunire e coordinare le attività esistenti e le nuove attività rilevanti. Qualsiasi strategia dovrebbe essere di proprietà di un'autorità adeguata ed essere sostenibile con le risorse umane e finanziarie necessarie. Tale quadro dovrebbe avere un mandato chiaro e un'autorità sufficiente attraverso un meccanismo (o consiglio) multi- stakeholder per coordinare tutte le attività relative ai diritti dei bambini, ai media digitali e all'ICT a livello intersettoriale, nazionale, regionale e locale, apprezzando gli sforzi esistenti nella definizione, coordinamento, attuazione e monitoraggio della strategia nazionale di protezione dei minori online.

Il documento dell'ITU propone delle azioni politiche mirate ad affrontare tutti i rischi e i potenziali danni per i bambini online e pensate per essere integrate da quadri più specifici come il modello *WePROTECT National Response (MNR)*[4] sullo sfruttamento e l'abuso sessuale dei bambini, che si concentra su danni specifici.

Le policy proposte sono suddivise per macroaree e vengono di seguito riassunte.

I diritti dei bambini

- Standardizzare la definizione di bambino come chiunque abbia meno di 18 anni in tutti i documenti legali in linea con l'articolo 1 della Convenzione delle Nazioni Unite sui diritti dell'infanzia (UN CRC).
- Costruire e collaborare con istituzioni indipendenti per i diritti umani per i bambini per garantire la protezione dei bambini online attraverso competenze specializzate, indagini e monitoraggio, promozione, sensibilizzazione, formazione e istruzione e con la partecipazione dei bambini.
- Includere la consultazione diretta con i minori, come è loro diritto ai sensi dell'articolo 12 della CRC delle Nazioni Unite, nello sviluppo, attuazione e

monitoraggio di qualsiasi tipo di quadro o piano d'azione per la protezione dei minori online.

Legislazione

- Riesaminare il quadro giuridico esistente per determinare l'esistenza di tutti i poteri giuridici necessari per consentire e assistere le forze dell'ordine e altri attori pertinenti per proteggere le persone di età inferiore ai 18 anni da tutti i tipi di danni online su tutte le piattaforme online.
- Stabilire che qualsiasi atto illegale contro un bambino nel mondo reale sia, "mutatis mutandis", illegale online e che le norme sulla protezione dei dati online e sulla privacy per i bambini siano adeguate.
- Allineare i quadri giuridici con gli standard internazionali esistenti, le leggi e le convenzioni relative ai diritti dei bambini e alla sicurezza informatica, facilitando la cooperazione internazionale attraverso l'armonizzazione delle leggi.
- Incoraggiare l'uso di una terminologia appropriata nello sviluppo della legislazione e delle politiche riguardanti la prevenzione e la protezione dello sfruttamento sessuale e dell'abuso sessuale dei bambini.

Forze dell'ordine

- Garantire che i casi di minori che danneggiano gli altri online siano trattati in linea con i principi dei diritti dei minori, opportunamente iscritti nella legislazione nazionale, favorendo fortemente strumenti diversi dal diritto penale.
- Fornire adeguate risorse finanziarie e umane, nonché formazione e rafforzamento delle capacità per coinvolgere pienamente ed equipaggiare la comunità delle forze dell'ordine.
- Garantire la cooperazione internazionale tra le forze dell'ordine in tutto il mondo, consentendo una risposta più rapida ai reati facilitati online.

Regolamentazione

- Considerare lo sviluppo di una politica di regolamentazione (sviluppo di politiche di coregolamentazione, quadro normativo completo).
- Imporre alle imprese l'obbligo di intraprendere una due diligence sui diritti dell'infanzia e di salvaguardare i propri utenti.
- Istituire meccanismi di monitoraggio per l'indagine e il risarcimento delle violazioni dei diritti dei bambini, al fine di migliorare la responsabilità delle TIC e di altre società pertinenti.
- Rafforzare la responsabilità dell'agenzia di regolamentazione per lo sviluppo di standard rilevanti per i diritti dei bambini e le TIC.

Monitoraggio e valutazione

- Istituire una piattaforma multi-stakeholder per guidare lo sviluppo, l'attuazione e il monitoraggio dell'agenda digitale nazionale per i bambini.
- Sviluppare obiettivi vincolati nel tempo e un processo trasparente per valutare e monitorare i progressi e garantire che le risorse umane, tecniche e finanziarie necessarie siano messe a disposizione per l'efficace funzionamento della strategia nazionale di protezione dei minori online e dei relativi elementi.

Industria delle ICT

- Coinvolgere l'industria nel processo di elaborazione delle leggi sulla protezione dei minori online e di metriche comuni per misurare tutti gli aspetti rilevanti della sicurezza online dei minori.
- Stabilire incentivi e rimuovere le barriere legali per facilitare lo sviluppo di standard e tecnologie comuni per combattere i rischi relativi ai contenuti per i bambini.
- Incoraggiare l'industria ad adottare un approccio di sicurezza e privacy fin dalla progettazione ai propri prodotti, servizi e piattaforme, riconoscendo il rispetto dei diritti dei bambini come obiettivo fondamentale.
- Garantire che l'industria utilizzi meccanismi rigorosi per rilevare, bloccare, rimuovere e segnalare in modo proattivo contenuti illegali e qualsiasi abuso (classificato come attività criminale) contro i bambini.
- Garantire che l'industria fornisca meccanismi di segnalazione adeguati e adatti ai bambini affinché i propri utenti possano segnalare problemi e preoccupazioni e possano ottenere ulteriore supporto.
- Collaborare con le parti interessate del settore per promuovere la consapevolezza al fine di supportare l'identificazione del settore rischi nello sviluppo e correggere prodotti e servizi esistenti. Ciò include la considerazione di altre preoccupazioni delle parti interessate e dei rischi e dei danni a cui sono esposti gli utenti finali.
- Supportare le parti interessate del settore affinché forniscano strumenti adatti all'età per aiutare i loro utenti a gestire meglio la protezione delle loro famiglie online.

Segnalazione

- Istituire e promuovere ampiamente meccanismi per segnalare facilmente i contenuti illegali trovati su Internet.
- Istituire un numero verde nazionale per l'infanzia con la capacità necessaria sui rischi e danni facilitati online o un numero verde per l'infanzia/un numero di assistenza per l'infanzia per facilitare la segnalazione da parte delle vittime di problemi di sicurezza online dei bambini.
- Istituire meccanismi di consulenza, segnalazione e reclamo sicuri e facilmente accessibili a misura di bambino.

Servizi sociali e assistenza alle vittime
- Garantire che siano in atto meccanismi di protezione dell'infanzia universali e sistematici che obblighino tutti coloro che lavorano con i bambini (ad es. assistenti sociali, operatori sanitari, educatori) a identificare, rispondere e segnalare qualsiasi tipo di danno ai bambini che si verifica online.
- Garantire che i professionisti dei servizi sociali siano formati sia per l'azione preventiva che per la risposta ai danni online ai minori, identificando gli abusi sui minori e fornendo un adeguato supporto specializzato e a lungo termine e assistenza ai minori, vittime di abusi.
- Sviluppare strategie e misure di prevenzione degli abusi sui minori basate su prove scientifiche.
- Fornire risorse umane e finanziarie adeguate a garantire il pieno recupero e reinserimento dei bambini e prevenire fenomeni di ricaduta (ri-vittimizzazione).
- Garantire che i bambini abbiano accesso a un'assistenza sanitaria adeguata (compresa la salute mentale e il benessere fisico) anche in caso di vittimizzazione, trauma o abuso online.

Raccolta e ricerca dati
- Effettuare ricerche sullo spettro degli attori nazionali e delle parti interessate per determinare le loro opinioni, esperienze, preoccupazioni e opportunità in merito alla protezione online dei minori.

Formazione scolastica
- Garantire che gli educatori e gli amministratori/professionisti scolastici siano formati per identificare e rispondere adeguatamente nei casi sospetti o confermati di minori vittime di abusi.
- Sviluppare un ampio programma di alfabetizzazione digitale adeguato all'età e incentrato su abilità e competenze per garantire che i bambini possano trarre pieno vantaggio dall'ambiente online, siano attrezzati per identificare le minacce e possano comprendere appieno le implicazioni del loro comportamento online.
- Sviluppare funzionalità di alfabetizzazione digitale come parte del curriculum scolastico nazionale che sia adeguato all'età e applicabile ai bambini fin dalla tenera età.
- Creare risorse educative al di fuori del curriculum scolastico che enfatizzino gli aspetti positivi e responsabilizzanti di Internet per i bambini e promuovano forme responsabili di comportamento online.
- Evitare i messaggi basati sulla paura.
- Consultare i bambini, nonché i genitori e gli accompagnatori sullo sviluppo di programmi, strumenti e risorse educative.

Consapevolezza e capacità nazionale
- Sviluppare campagne nazionali di sensibilizzazione del pubblico, che coprano un'ampia varietà di questioni che possono essere collegate all'ambiente digitale e adattate a tutti i gruppi target.
- Arruolare istituzioni pubbliche e mass media per la promozione di campagne nazionali di sensibilizzazione del pubblico.
- Sfruttare le campagne globali, nonché i quadri e le iniziative multistakeholder per creare campagne nazionali e rafforzare le capacità nazionali in materia di protezione online dei minori[5].

L'aspetto della privacy che coinvolge la tutela dei minori è stato trattato in ambito GDPR (Regolamento Privacy UE/2016/679) in diverse sezioni.

Il considerando 38 recita infatti: «I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore».

Esaminando più nello specifico, si sottolinea che l'articolo 8 dello stesso regolamento, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), contiene nuove e specifiche previsioni relative alle «Condizioni applicabili al consenso dei minorenni in relazione ai servizi della società dell'informazione», cui il nostro ordinamento dovrà adeguarsi con leggi nazionali. L'art. 8.1, in particolare, introduce la regola generale per cui il cd. "consenso digitale", applicato alla fornitura di servizi online per ragazzi under 18, sarà lecito solo laddove il minorenne "abbia almeno 16 anni".

Nel caso in cui, invece, l'interessato abbia un'età inferiore, il trattamento viene considerato lecito «soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale». Tuttavia, lo stesso art. 8.1 prevede una deroga al limite minimo di età per poter considerare valido il consenso rilasciato dal minorenne, precisando che «Gli Stati membri possono stabilire per legge un'età

inferiore a tali fini purché non inferiore ai 13 anni». Al riguardo si delineano diversi orientamenti: se da una parte l'accesso ad Internet offre ai bambini e ai giovani straordinarie opportunità di informazione, comunicazione e conoscenza portabile, immediata e globale, dall'altra li espone, attraverso l'accesso pressoché illimitato a contenuti, persone, luoghi virtuali, a rischi multiformi e complessi dai confini spesso labili e mutevoli.

L'entrata in vigore del GDPR, studiato per arginare i problemi legati alla privacy dell'individuo, ha avuto però un effetto collaterale che si è ripercosso sulla componente di cybersecurity della rete.

Se da un lato ha dettato norme per la protezione della privacy, dall'altro ha indotto gli operatori di registro ad oscurare i dati che confluivano nel WHOIS, dati che venivano utilizzati dalle forze dell'ordine e dagli operatori di cybersecurity come agevolazione nelle indagini sui crimini informatici.

Il tema della protezione dei minori online investe anche il sistema di assegnazione dei nomi a dominio gTLD - *generic Top Level Domain*. Nel momento in cui si discute di policy che riguardano i nomi a dominio, siano essi generici oppure specifici, non si può fare a meno di coinvolgere l'ente di gestione internazionale ICANN - *Internet Corporation for Assigned Names and Numbers*, il cui compito, tra gli altri, è quello di approvare e adottare le policy sull'assegnazione dei nomi a dominio e farle rispettare alle parti contraenti (*registries* e *registrars*) con ovvie ripercussioni sugli utenti finali.

In vista del *new round of gTLDs*, ovvero l'apertura di ICANN alla creazione di nuovi nomi a dominio di tipo generico, sono emerse tante preoccupazioni, una della quali riguarda proprio la tutela dei minori.

L'eNACSO - *European NGOs Alliance for Child Safety Online* ha seguito da vicino lo sviluppo delle policy sugli identificatori univoci di Internet e sul sistema di denominazione dei siti Internet coordinato da ICANN, dialogando con quest'ultimo e proponendo delle policy che regolano i domini generici di primo livello. eNACSO ha sollecitato ICANN al raggiungimento di un consenso sui ruoli e le responsabilità di tutti gli attori coinvolti nella governance di Internet e in particolare allo sviluppo un consenso sui ruoli e le responsabilità di quegli organismi dedicati a mantenere Internet sicuro, stabile e interoperabile.

In particolare, considerando l'impatto che il nuovo round di assegnazione di domini generici di primo livello (gTLD) ha sull'espansione e l'evoluzione di Internet, è stata messa in evidenza l'importanza di anteporre gli interessi dei bambini e dei giovani su quelli economici, specie quando si tratta di domini rivolti a loro o che attirino la loro attenzione (es: *.kid*, *.kids*, *.games*, *.juegos*, *.play*, *.school*, *.toys*...).

È stato richiesto ad ICANN di definire accordi sul funzionamento di tali gTLD, per garantire che i processi e le procedure siano ampiamente condivisi e concordati, tenendo presente che la sicurezza dei bambini dovrebbe avere la priorità.

eNACSO ha proposto lo sviluppo di linee guida e requisiti specifici che siano applicati a tutti i domini che si riferiscono espressamente a bambini e giovani, inclusa la richiesta di competenze specifiche da individui o organizzazioni con un background appropriato.

Il monitoraggio delle procedure di assegnazione dei gTLD con probabile impatto sui minori viene ad oggi seguito anche dal PSWG - *Public Safety Working Group* del GAC - *Governmental Advisory Committee*, che si occupa delle policy e delle procedure di sicurezza del web e che coinvolge, oltre che esponenti delle forze dell'ordine, i rappresentanti governativi di tutto il mondo[6].

4. Problema trattato a livello nazionale

Dalla questione internazionale si passa successivamente alla trattazione del problema a livello nazionale. Le istituzioni italiane che si occupano ad oggi della tutela dei minori in rete lavorano in sinergia per attuare le policy in linea con l'ambiente internazionale.

La prima tra tutte l'Autorità Garante per l'Infanzia e l'Adolescenza (AGIA) che tratta l'argomento in modo approfondito nel documento *La tutela dei minorenni nel mondo della comunicazione* con un'apposita sezione minorenni e web.

L'AGIA sottolinea l'importanza dell'educazione digitale, focalizzando l'attenzione sulla «capacità di essere soli e non in continua comunicazione» come contrasto alla soluzione alla *dipendenza* menzionata in precedenza.

Insiste sulla cultura della sicurezza, evidenziando la sussistenza in rete di siti Internet i cui contenuti si scontrano con i principi basilari di tutela dei minori, quali siti che esaltano le pratiche di anoressia e bulimia (c.d. "pro-ana" e "pro-mia") e siti che istigano al suicidio e all'autolesionismo ("cutting").

Persiste, secondo l'AGIA, l'esigenza di bilanciare diversi diritti fondamentali menzionati nel trattato internazionale che regola i diritti civili, politici, economici, sociali, culturali dei bambini (*Convention on the Rights of the Child* - CRC). Tra questi diritti vi sono: la tutela dei minorenni nell'ambito dell'uso sicuro delle tecnologie dell'informazione (articolo 17),

il diritto all'informazione e la libertà di espressione (articolo 13); l'obbligo degli Stati di garantire ai genitori di poter svolgere congiuntamente il loro diritto/dovere di proteggere e educare i figli (articolo 18); il diritto di essere protetti da abusi sessuali (articolo 34).

Emerge la necessità di continuo aggiornamento legislativo e l'affinamento delle tecniche investigative e repressive, promuovendo quindi un'azione preventiva che coinvolga la famiglia, le istituzioni, le varie agenzie educative e le organizzazioni che si occupano dell'infanzia e dell'adolescenza che hanno la responsabilità di far sperimentare alle nuove generazioni una dimensione di cittadinanza in cui esercitare "consapevolmente" libertà, responsabilità e democrazia.

È chiaro come i numerosi input provenienti anche dalla UE in materia di crescita "digitale" includono temi importanti e significativi in ordine alla protezione dei minorenni dai rischi connessi alle nuove tecnologie. Fra di essi necessita di menzione il concetto di "consenso digitale", il quale si impone quale tema prodromico ad una tutela che trovi la giusta mediazione tra il diritto di accesso alla rete e il rispetto di altro importante diritto che è quello di una protezione potenziata, in ragione della peculiare fragilità dell'infanzia e dell'adolescenza[7].

Come già anticipato, la sinergia tra le istituzioni è fondamentale per affrontare un argomento così complesso e delicato. Riguardando il mondo delle comunicazioni, il coinvolgimento dell'Autorità Garante delle Comunicazioni (AGCOM) è stato fondamentale nella stesura di diversi provvedimenti e delibere in materia di tutela dei minori online.

Con la delibera n. 481/14/CONS del 23 settembre 2014, l'AGCOM ha istituito l'Osservatorio permanente delle forme di garanzia e di tutela dei minori e dei diritti fondamentali della persona sulla rete Internet al fine di analizzare le problematiche connesse all'utilizzo di Internet e dei social network e di verificare l'efficacia delle procedure adottate dagli operatori.

L'osservatorio si muove seguendo due linee direttrici:

1. la raccolta, l'elaborazione e la pubblicazione dei dati relativi al comportamento degli utenti rispetto a Internet e ai social network;
2. l'analisi delle policies adottate dagli operatori per la salvaguardia dei valori e degli utenti più sensibili e la valutazione della relativa efficacia e ha come oggetto di monitoraggio fenomeni quali: l'istigazione all'odio, le minacce, le molestie, il bullismo, l'hate speech e la diffusione di contenuti deplorevoli.

L'iniziativa dell'AGCOM incentra le sue basi su un quadro giuridico che fa riferimento alle competenze in ambito di tutela dei minori:

- la legge istitutiva (art. 1, comma 6, lett. b), n. 6 della legge n. 249/97): competenza specifica in materia di tutela dei minori (con attribuzione di ruolo specifico anche all'autoregolamentazione e alla co-regolamentazione);
- il Testo unico dei servizi di media audiovisivi e radiofonici: principi fondamentali del sistema radiotelevisivo e rispetto per la dignità umana (art. 32, comma 5);
- il decreto legislativo 9 aprile 2003, n. 70: l'Autorità amministrativa competente può limitare la libera circolazione di un determinato servizio della società dell'informazione proveniente da un altro Stato membro «per l'opera di prevenzione, investigazione, individuazione e perseguimento di reati, in particolare la tutela dei minori e la lotta contro l'incitamento all'odio razziale, sessuale, religioso o etnico, nonché contro la violazione della dignità umana» (Art. 5, comma 1, lett. a).

Anche le autorità di *law enforcement* si sono adoperate nello sviluppo di linee guida e best practice per il contrasto dei fenomeni criminali che si sviluppano nel mondo virtuale coinvolgendo i minori.

Una fra tutte, la pubblicazione di un contributo concreto sulla navigazione sicura e consapevole dei minori su Internet, sviluppato in collaborazione di altre istituzioni ministeriali, che coinvolge i genitori e fornisce loro alcuni strumenti pratici per la formazione, la prevenzione e il monitoraggio.

Un ruolo importante è sicuramente quello del monitoraggio, esaminato dal punto di vista prettamente pratico e di facile comprensione, nel quale vengono esaminati i tipici comportamenti che evidenziano anomalie e devono far scattare il campanello d'allarme al tutore[8].

Il Ministero dello Sviluppo Economico ha espresso la sua posizione sottolineando l'importanza, in un panorama mediatico sempre più ibrido e integrato, del rispetto dell'equilibrio tra la dimensione produttiva-economica e quella etica e delle implicazioni dei messaggi mediali sui minori. Per questo, alla luce dei cambiamenti che portano verso contesti sempre più digitali, occorre l'impegno di tutte le istituzioni coinvolte per allineare la normativa italiana in materia di minori alle sfide poste dai nuovi linguaggi multimediali[9].

5. Conclusioni

Le strategie Europee e Nazionali sono in continua evoluzione per far fronte a minacce sempre più evo-

lute e mutevoli. Una collaborazione istituzionale che si spinga fino al livello locale, coinvolgendo le scuole e le forze dell'ordine può essere una buona pratica per arginare il problema creando un clima di fiducia da parte del minore nei confronti dei formatori.

Questo intervento a livello scolastico però non basta. Molto spesso viene sottovalutato l'ambiente extrascolastico, dove i minori trascorrono la maggior parte del loro tempo. Per questo motivo assumono una particolare rilevanza le iniziative volte al coinvolgimento dei genitori e dei tutori in un processo di apprendimento studiato *ad hoc* per loro. Tale processo dovrebbe includere una formazione di base all'utilizzo dei dispositivi digitali e delle principali tecniche di prevenzione e controllo del traffico dati sul web, oltre che spingere i genitori e i tutori ad acquisire un maggiore spirito di osservazione riguardo i comportamenti dei minori e dell'ambiente virtuale che essi sono abituati a frequentare.

L'*awareness* diventa la parola chiave per affrontare le sfide di un mondo virtuale la cui rapidità di evoluzione viene spesso sottovalutata anche dagli addetti ai lavori.

Note

[1]Cfr. European Commission, *European Strategy for a better Internet for our children*, 2021.

[2]United Nations - Human Rights - Office of the High Commissioner, *Convention of the Rights of the Child*, 1990.

[3]United Nations - Committee on the Rights of the Child, *General comment No. 25 (2021) on children's rights in relation to the digital environment*, 2021.

[4]WeProtect Global Alliance, *Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response*, 2016.

[5]Si veda ITU Policy Brief, *Keeping children safe in the digital environment: The importance of protection and empowerment*, 2021.

[6]eNACSO - European NGOs Alliance for Child Safety Online, *The rules governing General Top-Level Domains*.

[7]Autorità Garante per l'Infanzia e l'Adolescenza, *La tutela dei minorenni nel mondo della comunicazione*, 2017.

[8]Si veda Commissariato di P.S. on line, *Per i genitori. Navigazione sicura e consapevole dei minori su internet*.

[9]Cfr. Ministero dello sviluppo economico, *Avviato percorso condiviso per la tutela dei minori sulle multipiattaforme digitali*, 2020.

* * *

Internet: When the net catches children

Abstract: The child online protection is a complex issue that involves institutions of all levels in cascade. There are many initiatives of policies and best practices definition to try to stem the phenomena connected to the relationship, actually unhealthy, that children have with the digital world, with which they become familiar even before schooling. Digital education must be addressed in a capillary way starting from the legislator to the educator, the latter often too slow to keep up with the frenzy of the network to which the new generations are subjected. This paper briefly summarizes some of the main threats present on the net and their repercussions on the health of minors, offering an overview of some of the strategic initiatives undertaken at European and national level, in order to underline the importance of training and prevention at any educational level.

Keywords: Children – Cyberbullying – Strategy – Protection – Abuse