Generazioni Connesse
SAFER INTERNET CENTRE

Co-funded by the European Union

# SINERGIE DIGITALI: DIALOGHI TRA LO YOUTH PANEL DEL PROGETTO GENERAZIONI CONNESSE - SIC E LE ISTITUZIONI

REPORT DELLE CRITICITA' E PROPOSTE EMERSE

## INTRODUZIONE

La Direzione Generale per lo Studente, l'Inclusione e l'Orientamento Scolastico del Ministero dell'Istruzione e del Merito coordina, dal 2012, il progetto Safer Internet Centre – Generazioni Connesse. Tale progetto è realizzato in collaborazione con rilevanti partner istituzionali e privati impegnati nella promozione della sicurezza online.

Il Safer Internet Centre (SIC) in collaborazione con il Giffoni Film Festival**,** ha istituito un gruppo di 40 giovani esperti—ragazzi e ragazze di età compresa tra i 15 e i 19 anni, provenienti da nord, centro e sud Italia —che costituiscono il cosiddetto Youth Panel.

Lo Youth Panel svolge un ruolo fondamentale nel supportare le iniziative del Centro Italiano per la Sicurezza in Rete. La sua missione è fornire una *youth rights-based perspective* sull'uso positivo e responsabile delle tecnologie digitali partecipando attivamente a eventi di formazione e sensibilizzazione a livello nazionale e internazionale, promuovendo campagne di sensibilizzazione rivolte ai loro pari e agendo come portavoce delle istanze e delle opinioni dei giovani presso le istituzioni italiane e la Commissione Europea.

Nell'ambito delle attività previste dal progetto SIC 2024-2025, lo Youth Panel ha organizzato una tavola rotonda, cui fa riferimento il presente rapporto. L'evento, svoltosi il 24 luglio 2024, ha riunito lo Youth Panel del Safer Internet Centre italiano e i principali attori istituzionali del Paese, tra cui l'Agenzia per la Cybersicurezza Nazionale (ACN), l'Autorità per le Garanzie nelle Comunicazioni (Agcom), l'Autorità Garante per l'Infanzia e l'Adolescenza (AGIA), il Dipartimento per le Politiche della Famiglia (DIPOFAM), il Garante per la Protezione dei Dati Personali (GPDP) e la Polizia Postale.

La discussione si è concentrata sui ruoli e responsabilità istituzionali in materia di *online safety*, con particolare attenzione alla protezione dei più giovani e all'educazione all'uso consapevole degli ambienti digitali. Sono state inoltre discusse le criticità rilevate nell'analisi degli ambienti digitali e le azioni concrete che giovani e istituzioni possono promuovere e realizzare insieme.

**Obiettivi**

L'incontro mirava a fornire una piattaforma di dialogo tra i giovani dello Youth Panel e le istituzioni, permettendo ai partecipanti di portare avanti proposte concrete e lavorare insieme per migliorare la sicurezza online e il benessere digitale dei più giovani.

**Focus**

La sessione si è concentrata sui seguenti punti;

- Ruoli e responsabilità delle istituzioni in relazione alla sicurezza online dei più giovani.
- Criticità rilevate e proposte di azioni concrete da realizzare.

**Metodologia**

La metodologia di lavoro proposta ha integrato i seguenti quattro assi tematici, sui quali i/le giovani si sono confrontati e preparati all'interno di quattro sessioni formative online e una in presenza con il supporto degli/delle esperti/e del SIC:

1. *Asse "Benessere Digitale"* attraverso cui si è analizzato l'impatto delle tecnologie e dei servizi digitali sulla salute mentale, fisica, sociale ed emotiva di ragazzi e ragazze.
2. *Asse "Privacy e Sicurezza"* attraverso cui si sono analizzati il tema del consenso negli ambienti digitali, la raccolta e utilizzo dei dati di bambini e ragazzi e l'internet business model.
3. *Asse "e-Democracy e e-Governance"* attraverso cui si sono analizzati i temi della libertà di informazione e della disinformazione (fake news).

4. *Asse "Etica dell'Intelligenza Artificiale"* attraverso cui si sono analizzati i bias algoritmici e i processi di automazione.

**Questi temi sono stati trattati in relazione al Digital Services Act e alla strategia BIK+, creando un quadro completo e interdisciplinare per la discussione.**

Il Digital Services Act è stato presentato e approfondito specificamente riguardo ai diritti online dei minori durante la prima sessione formativa, così come i ruoli, i mandati e le funzioni di ciascuno degli attori istituzionali che lo Youth Panel incontrerà al Giffoni Film Festival.

Successivamente, lo Youth Panel è stato suddiviso in quattro gruppi di lavoro, ciascuno guidato da un/una esperto/a del SIC, al fine di elaborare riflessioni, evidenziare criticità e proporre soluzioni, basandosi sugli assi tematici e sui mandati di ciascun attore istituzionale.

Il presente rapporto documenta dunque il lavoro svolto e le questioni emerse che hanno costituito i punti focali della discussione, oltre alle proposte formulate, per le quali lo Youth Panel ha richiesto un impegno alle istituzioni.

In taluni casi ove indicato, le criticità individuate, le domande e le proposte sono rivolte a un singolo attore istituzionale, in linea con le sue funzioni e il suo mandato. In altri, le proposte coinvolgono responsabilità che riguardano due o più attori. Altre ancora costituiscono domande aperte rivolte a tutti gli attori invitati al confronto.

## DOMANDE E PROPOSTE PER AGCOM E GPDP

### TEMA: TAVOLO CONGIUNTO AGCOM- GPDP SU AGE VERIFICATION

ASSI INTERESSATI: BENESSERE DIGITALE/PRIVACY/ETICA IA/DSA

Garante Privacy e AGCOM hanno istituito un tavolo congiunto, finalizzato alla promozione di un codice di condotta che conduca le piattaforme digitali ad adottare sistemi per la verifica dell'età dei più giovani che accedono ai servizi online. I rischi per i giovanissimi che usano servizi digitali sono enormi e noti da tempo; è difficile, peraltro, individuare soluzioni affidabili per l'age verification. L'istituzione del tavolo, oltre a consentire auspicabilmente di pervenire alla soluzione del problema, permetterà alle due Autorità di iniziare a sperimentare forme di cooperazione nella tutela degli utenti di servizi digitali. L'istituzione del tavolo è stata ufficializzata nel marzo 2023 con la firma del protocollo d'intesa, con cui il Garante e l'Agcom si sono impegnati a dare vita ad una serie di iniziative utili allo svolgimento dei rispettivi compiti, mediante lo scambio di dati e informazioni, la creazione di gruppi di studio e il lancio di consultazioni pubbliche congiunte. Il protocollo ha durata annuale e prevede la cooperazione su temi di interesse comune per l'applicazione della normativa europea e nazionale vigente o di prossima attuazione. Tra essi, è già in programma un'indagine conoscitiva sul fenomeno della pubblicità politica mirata attraverso tecniche di profilazione.

### DOMANDE PER AGCOM E GDPD

1. **Sistemi di Age Verification**
   - Quali sono i criteri utilizzati per valutare l'efficacia dei sistemi di age verification?
   - Quali potrebbero essere i possibili rischi legati alla privacy derivanti dall'adozione di sistemi di age verification?
   - Se e in che modo sono state/saranno coinvolte le piattaforme digitali nel processo di definizione del codice di condotta?
2. **Implementazione di soluzioni tecnologiche avanzate**

- Se e in che modo si è esplorato l'uso di tecnologie avanzate, come l'intelligenza artificiale e il machine learning, per migliorare l'affidabilità dei sistemi di verifica dell'età?

3. **Coinvolgimento del pubblico**
   - Se e in che modo le consultazioni pubbliche sono state/saranno strutturate per assicurare un'ampia partecipazione e rappresentanza delle diverse voci della società, ivi incluse quelle dei più giovani?
   - Quali meccanismi sono stati/saranno messi in atto per raccogliere e integrare i feedback di genitori, docenti, educatori?
4. **Indagine sulla pubblicità politica mirata**
   - Quali sono gli obiettivi specifici dell'indagine conoscitiva sulla pubblicità politica mirata?

### PROPOSTE PER AGCOM E GDPD

1. **Sviluppo di Linee Guida**
   - Lo Youth Panel propone lo sviluppo di linee guida chiare e dettagliate per le piattaforme digitali, che includano requisiti tecnici e di sicurezza per la verifica dell'età.
2. **Campagne di sensibilizzazione**:
   - Lo Youth Panel propone di avviare campagne di sensibilizzazione congiunte AGCOM- GPDP rivolte a genitori, insegnanti e minori stessi sull'importanza della verifica dell'età e dei rischi associati all'uso dei servizi digitali senza adeguate protezioni.
   - Lo Youth Panel si propone di collaborare con AGCOM e GPDP per diffondere informazioni utili e strumenti pratici per la protezione online dei minori.

## DOMANDE E PROPOSTE PER AGCOM

### TEMA: PARENTAL CONTROL E DELIBERA 9/23/CONS

ASSI INTERESSATI e-DEMOCRACY/BENESSERE DIGITALE/PRIVACY

Il 21 novembre 2023 sono entrate in vigore le nuove regole dell'Autorità per le Garanzie delle Comunicazioni (Agcom) riguardanti la tutela dei minori sul web. In particolare, la delibera 9/23/CONS di gennaio 2023 prevede che gli operatori di telecomunicazioni forniscano gratuitamente sistemi di parental control ai propri utenti. Nel concreto significa che i fornitori di servizi web, al momento dell'acquisto di una nuova sim o della sottoscrizione di un nuovo contratto, devono includere un sistema che blocchi (o dia l'opzione di bloccare) una serie di contenuti ritenuti inappropriati (tra cui pornografia, gioco d'azzardo, vendita di armi, violenza, autolesionismo, discorsi d'odio, pratiche dannose per la salute, e strumenti per rendere l'attività online irrintracciabile), a cui i minori non potranno avere accesso. Qualora il contratto sia intestato a una persona minorenne, il filtro viene applicato in automatico. Le indicazioni sono preliminari e gli operatori devono comunicare i contenuti da bloccare e le soluzioni tecniche adottate. Agcom ha indicato gli obiettivi ma ha lasciato la scelta dei mezzi agli operatori.

### CRITICITÀ EMERSE

Le categorie di contenuti da bloccare sono state identificate attraverso una consultazione pubblica con associazioni di categoria, operatori, associazioni dei consumatori e organizzazioni di genitori (anche con orientamenti politici ben chiari). **Le criticità riguardano la delega ai privati per la definizione dei siti pericolosi**. Ci sono preoccupazioni sulla **vaghezza delle categorie vietate e il rischio di censura e disinformazione**. **Bilanciamento tra diritto all'informazione e protezione dei più giovani**.

### DOMANDE PER AGCOM

**Implementazione dei sistemi di Parental Control**

- Quali criteri sono stati utilizzati per scegliere i sistemi di parental control forniti gratuitamente dagli operatori?
- Come viene monitorata l'efficacia di questi sistemi nel bloccare i contenuti inappropriati?
- Sono previsti meccanismi di revisione e aggiornamento dei sistemi di parental control per garantire che rimangano efficaci nel tempo?

**Definizione dei contenuti da bloccare**

- Come vengono aggiornate le categorie di contenuti da bloccare in risposta ai cambiamenti del panorama digitale e dei nuovi rischi online?
- Quali misure vengono prese per garantire che i criteri utilizzati per identificare i contenuti inappropriati siano trasparenti e comprensibili?

**Criteri per definire le categorie dei contenuti da bloccare**

- Quali criteri specifici sono utilizzati per evitare interpretazioni troppo ampie e vaghe delle categorie di contenuti vietati?

**Delega ai privati**

- Quali misure sono in atto per garantire che la delega ai privati nella definizione dei siti pericolosi non porti a censura ingiustificata?
- Come si intende affrontare la questione del potere discrezionale che viene affidato ai fornitori di servizi esterni?

**Consultazioni pubbliche**

- Se e come è stata garantita un'ampia rappresentanza delle diverse voci della società e di bambini/e, ragazzi/e nelle consultazioni pubbliche?

## PROPOSTE PER AGCOM

**Trasparenza e comunicazione:**

- Pubblicare periodicamente report dettagliati sui risultati ottenuti con l'implementazione dei sistemi di parental control, includendo statistiche su contenuti bloccati e feedback degli utenti.
- Creare un portale dedicato dove genitori ed educatori possano trovare informazioni aggiornate e risorse utili per proteggere i minori online.

**Revisione e aggiornamento continui**

- Istituire un comitato di esperti indipendenti che possa revisionare periodicamente le categorie di contenuti da bloccare e proporre aggiornamenti basati su nuovi rischi e minacce digitali.

**Coinvolgimento delle parti interessate**

- Organizzare workshop/incontri con la partecipazione di esperti, operatori, associazioni dei consumatori e organizzazioni di genitori per discutere e migliorare le misure di tutela dei minori.
- Incentivare la collaborazione con scuole, docenti, oltre che con lo Youth Panel del SIC, per sensibilizzare i minori sui rischi online e sulle buone pratiche di online safety.

**Monitoraggio e valutazione**

- Implementare un sistema di monitoraggio continuo per valutare l'efficacia dei sistemi di parental control e apportare modifiche basate sui dati raccolti.

**Protezione dei diritti e della libertà di espressione**

- Stabilire linee guida chiare per evitare che la definizione dei contenuti da bloccare possa portare a censure ingiustificate o limitazioni della libertà di espressione.
- Garantire che le decisioni sui contenuti da bloccare siano basate su criteri oggettivi e verificabili, evitando interpretazioni soggettive o arbitrarie

## DOMANDE E PROPOSTE PER GPDP

### TEMA: SEGNALAZIONI IN MATERIA DI CYBERBULLISMO E REVENGE PORN

ASSI INTERESSATI: PRIVACY E SICUREZZA

Il gruppo di lavoro "Privacy and Safety", tra le varie tematiche oggetto di approfondimento, ha avuto modo di analizzare gli strumenti di segnalazione attualmente a disposizione dei ragazzi. Più in particolare, le attività si sono focalizzate sugli strumenti resi disponibili dal Garante Privacy per la segnalazione di casi di revenge porn e cyberbullismo. Nel corso dei lavori è emerso come l'efficacia degli strumenti di segnalazione e reclamo sia strettamente correlata alla velocità di intervento e di adozione di misure di contrasto. La portata negativa di entrambi i fenomeni - cyberbullismo e revenge porn - è infatti strettamente correlata alla "viralità" che caratterizza i contenuti postati e alla persistenza online di tali contenuti. Altro aspetto di particolare interesse ha riguardato la possibilità per gli ultraquattordicenni di poter attivare i sistemi di segnalazione e reclamo in maniera del tutto autonoma ed a prescindere dall'intervento di genitori/tutori, ciò in base all'art. 2 della L. 71/2017 (per il Cyberbullismo) ed all'art. 144 bis del Codice Privacy (per il Revenge Porn).

Secondo i dati emersi nella recente relazione annuale, nel 2023, al Garante Privacy sono giunte circa 650 segnalazioni in materia di revenge porn, a fronte delle quali l'Autorità ha adottato 299 provvedimenti d'urgenza. Il confronto con i dati del 2022 fanno emergere un raddoppio delle segnalazioni.

I membri dello Youth Panel pur ritenendo assolutamente apprezzabile ciò che è stato realizzato, hanno voluto apportare un proprio contributo per evidenziare alcuni aspetti critici e, nel contempo, per lanciare delle proposte.

### CRITICITÀ EMERSE

Rispetto ai due canali di segnalazione sono state rilevate delle differenze nelle procedure:

- per quanto riguarda la segnalazione di casi di cyberbullismo, l'Autorità nella pagina dedicata, mette a disposizione un file word che ciascun utente deve scaricare, compilare e trasmettere come allegato mail all'indirizzo cyberbullismo@gpdp.it . L'utilizzo di un "Modello" comporta il rischio che il segnalatore (soprattutto se nella fascia 14-18 anni) possa omettere degli elementi essenziali per consentire al Garante di agire in maniera rapida ed efficace. Inoltre la necessità di download del modello, compilazione ed inoltro appare eccessivamente "macchinosa";

- in relazione alla segnalazione di casi di revenge Porn, il sito del Garante Privacy, consente una duplice possibilità:
    a. gli utenti non autenticati devono compilare ed inviare un modulo, e poi seguire le istruzioni che riceveranno sulla loro casella di posta;
    b. gli utenti possono autenticarsi tramite SPID, CIE o EIDAS e completare la propria segnalazione interamente online.

Sicuramente è molto utile avere un percorso di segnalazione con campi vincolati, tuttavia per gli utenti non autenticati, il doppio passaggio, con l'attesa delle istruzioni da seguire, può scoraggiare l'utente segnalatore. Per quanto riguarda invece il criterio di autenticazione è necessario considerare che la maggioranza degli utenti minorenni ultraquattordicenni non ha la possibilità di utilizzare SPID, CIE o EIDAS.

### DOMANDE PER GDPD

- Quali possono essere gli ulteriori strumenti e modalità per rendere autonomi i minori ultraquattordicenni nell'effettuare le segnalazioni?
- È possibile prevedere che il minore che segnali un abuso sia ricontattato telefonicamente da un operatore, così da fornire un feedback immediato e "umano"?
- È possibile avere una stima delle segnalazioni da parte di utenti non autenticati che poi non sono state portate a termine?

### PROPOSTE PER GDPD

Per quanto concerne la reperibilità dei sistemi di segnalazione **sarebbe opportuno creare un unico punto "Segnalazioni" nella homepage del sito del Garante Privacy, che smisti gli utenti sulle varie sezioni specifiche** (cyberbullismo, revenge porn, ecc.).
Dal punto di vista operativo si suggerisce di **strutturare i moduli di segnalazione in maniera unitaria, e preferibilmente utilizzando solo moduli online con campi vincolati**.

## DOMANDE E PROPOSTE PER DIPOFAM

### TEMA: SHARENTING

ASSI INTERESSATI: PRIVACY E SICUREZZA

Il gruppo di lavoro "Privacy and Safety", nel corso delle attività di lavoro ha considerato il fenomeno dello sharenting analizzando lo stato attuale e confrontandosi su quali potranno essere le ricadute in futuro. A parere del gruppo di lavoro ancora non è possibile avere piena contezza di quali conseguenze saranno generate negli anni a venire dalla sconsiderata diffusione di contenuti (prevalentemente video e immagini) riferite a minori ed attuata dai loro genitori. Attività di webscraping illecite così come l'utilizzo per finalità criminose di tali contenuti potrebbero seriamente compromettere l'identità in rete dei bambini di oggi.

### CRITICITÀ EMERSE

Nel corso dei lavori è emerso che il fenomeno dello sharenting, per le sue specifiche caratteristiche, risulta essere scarsamente reattivo rispetto a misure di carattere "coercitivo". Troppo spesso i genitori considerano i propri figli come una "proprietà privata" sulla quale hanno qualsiasi potere, e con la stessa frequenza il "figlio-oggetto" viene mostrato in rete senza alcun tipo di cautela. A fronte di tali azioni, con tutta probabilità, divieti o sanzioni di varia natura non sortirebbero alcun effetto, in quanto alla base dello sharenting c'è una diffusa ignoranza rispetto ai rischi tecnologici da un lato, e rispetto ai diritti che spettano anche ai figli in quanto esseri umani. Sono diverse le sentenze mediante le quali alcuni giudici italiani hanno imposto ai genitori la rimozione di immagini e video aventi ad oggetto i propri figli, vietando anche le future pubblicazioni. Si tratta in questi casi di rimedi estremi e che non risolvono il problema a monte, è necessario lavorare sulla cultura del rispetto e della legalità anche in questo ambito.

### DOMANDE PER DIPOFOAM

- Quali sono le iniziative di contrasto allo sharenting adottate fino ad oggi?
- Sareste favorevoli ad una campagna pubblicitaria di impatto destinata ai genitori sul modello di altri paesi? (esempio)

### PROPOSTE PER DIPOFOAM

- La realizzazione di campagne informative massive (spot pubblicitari, campagne social media, ecc), e l'organizzazione di corsi di sensibilizzazione per i genitori, potrebbero rappresentare un buon punto di partenza.
- Altrettanto importante potrebbe essere la realizzazione di corsi più specifici con campagne del tipo "Patentino del genitore tecnologico".

## DOMANDE E PROPOSTE PER ACN

### TEMA: CYBERSECURITY: UNO SCUODO DIGITALE PER IL NOSTRO PAESE

ASSI INTERESSATI: PRIVACY E SICUREZZA

Navigando il sito dell'ACN salta agli occhi una frase in particolare: "In un mondo sempre più digitalizzato e connesso, la cybersicurezza è diventata di fondamentale importanza". Questa affermazione sintetizza molti aspetti del mondo attuale, digitalizzato, globalizzato, dove tutte le attività, da quelle quotidiane dei cittadini a quelle particolarmente sensibili delle istituzioni, sono effettuate in rete. Lasciando da parte il settore della criminalità informatica comune, quella delle piccole truffe, oggi notiamo un livello superiore di attacchi informatici che, in molti casi, potrebbero mettere in ginocchio l'intero paese. Allo scoppio dell'attuale conflitto in Ucraina c'è stata una corsa all'implementazione di sistemi di sicurezza informatici sempre più sofisticati, proprio perché oggi anche le guerre viaggiano su internet.

#### CRITICITÀ EMERSE

Come detto in premessa, all'ACN deve essere necessariamente riconosciuto un ruolo fondamentale nel nostro paese. Sebbene si tratti di un'Autorità "giovane", essendo stata istituita appena quattro anni fa, noi giovani non abbiamo ancora avuto tante occasioni di conoscerla. Attualmente l'ACN sta assumendo molti giovani professionisti con competenze elevate e riteniamo che in futuro tali figure professionali saranno sempre più richieste. A differenza di altre autorità, non ci risulta che siano state effettuate attività di presentazione e sensibilizzazione nel contesto scolastico.

#### DOMANDE PER ACN

- È ipotizzabile in futuro la realizzazione di una vera e propria "accademia della cybersecurity", con la quale formare i massimi esperti, e dalla quale le istituzioni possano attingere le figure professionali necessarie? Si tratterebbe di mutuare in un certo senso l'esperienza della Scuola superiore dell'amministrazione.

#### PROPOSTE PER ACN

- Così come avviene per altre istituzioni, sarebbe auspicabile che, di concerto con il MIM, siano attivate delle campagne di informazione e formazione nelle scuole, per far meglio conoscere l'ACN.
- Per gli istituti secondari di secondo livello potrebbe essere interessante illustrare, soprattutto agli studenti che hanno maggiori attitudini rispetto al settore informatico, quali possono essere gli sbocchi lavorativi nel settore della cybersecurity.

## DOMANDE E PROPOSTE PER POLIZIA POSTALE, GPDP E AGIA

### TEMA: IL DIRITTO ALLA PRIVACY, ALL'IMMAGINE, E VIOLENZA DI GENERE ONLINE

ASSI INTERESSATI: e-DEMOCRACY/BENESSERE DIGITALE/PRIVACY/ETICA IA

Abbiamo riflettuto sul fenomeno crescente di deepfake e deepnude, e di come possano essere un rischio altissimo per minori. Abbiamo fatto ricerca su normativa vigente, su eventuali lacune, e di come dobbiamo puntare sulla prevenzione.

Secondo un articolo del sito Diritto dell'Informatica, il Garante della Privacy aveva aperto nel 2020 un'istruttoria nei confronti di Telegram, poiché su un canale dell'app di comunicazione circolava una foto manipolata di una ragazza senza vestiti.

Infatti, compaiono sempre più siti di pubblicazione di deepnude e deepfake, e app di manipolazione, per cui da una foto di una persona, se ne può creare un'altra senza indumenti. Secondo l'articolo: "*Quanto accaduto ha dato il via a molteplici riflessioni sui possibili risvolti negativi di un'eventuale diffusione incontrollata delle immagini così prodotte, a partire dalle potenziali gravi lesioni alla dignità e alla privacy dei soggetti, nonché del possibile rischio che le stesse vengano utilizzate a fini estorsivi o di revenge porn*."

Siccome sia deepfake che deepnude possono intaccare la dignità di una persona, si potrebbero prevedere dei diritti precisi in merito. Tuttavia, secondo Forensic News, l'attuale Codice penale non prevede una specifica norma dedicata ad immagini creati mediante l'intelligenza artificiale, e c'è incertezza in merito all'affermare nello specifico, se chi si rende autore di un reato di questo genere potrebbe essere accusato di sostituzione di persona (art. 494 c.p.), e di frode informatica (art. 640ter, comma III, c.p.). I minori nello specifico sono protetti da illeciti commessi tramite deepfake e deepnude, secondo il codice penale (art. 600quater, comma I, c.p. che disciplina il reato di pornografia virtuale). Abbiamo riflettuto sulla possibilità di usare modelli di IA per "combattere" questi fenomeni, ossia usarli per l'identificazione di video e immagini alterate, e di APP che ne permettono la creazione. Però, secondo NPR, è una soluzione complicata, in quanto i modelli di creazione diventano sempre più complessi e sofisticati, per cui l'identificazione potrebbe risultare difficile.

## DOMANDE PER POLIZIA POSTALE

- Quali sono le principali sfide e difficoltà incontrate dalla Polizia Postale nel contrastare la diffusione di deepfake e deepnudes che coinvolgono minori?
- Quali sono gli strumenti e le tecnologie impiegate dalla Polizia Postale per individuare e contrastare la produzione e la diffusione illecita di materiale deepnudes che coinvolge minori?
- Quali sono le strategie e le risorse messe in atto per educare i minori sui rischi legati alla manipolazione digitale e al fenomeno dei deepfake?
- Come viene gestito e affrontato il caso di minori vittime di deepfake o deepnudes in termini di supporto psicologico e legale?

## PROPOSTE PER POLIZIA POSTALE

- Prevedere una sessione ad hoc con consigli per ragazzi/e, genitori, sui rischi derivanti dai deepfake e deepnudes sul sito: https://www.commissariatodips.it/approfondimenti/pedofilia-online/pedofilia-on-line-che-cose/index.html
- Come già previsto dal progetto Generazioni Connesse prevedere momenti di collaborazione ad hoc tra lo Youth Panel e il truck della Polizia Postale al fine di approfondire contenuti specifici di maggior interesse per ragazzi/e (ad esempio sulla privacy o su deepnudes, deepfakes) negli appuntamenti.

## PROPOSTA PER TUTTI GLI ATTORI ISTITUZIONALI

- La nostra richiesta è di proporre alle istituzioni di usare modelli regolamentati di AI nel processo di ricerca dei deepfake e deepnude (sia APP per la creazione, che siti di pubblicazione), per automatizzare il processo di identificazione, e identificare altre soluzioni già in atto in merito. Vogliamo riflettere sulla possibilità di creare una normativa specifica rispetto a deepfake e deepnude, e dialogare con le istituzioni sull'importanza della prevenzione, tramite interventi di educazione all'affettività nelle scuole (Diritto Penale Uomo).

## DOMANDE E PROPOSTE TRASVERSALI A TUTTI GLI ATTORI ISTITUZIONALI

### TEMA: BENESSERE DIGITALE

ASSI INTERESSATI: e-DEMOCRACY/BENESSERE DIGITALE/PRIVACY/ETICA IA

Lo Youth Panel ha avviato un confronto interno sul Benessere Digitale già in occasione del Back to school 2023 in cui ha avuto l'occasione di incontrare e dialogare con tre grandi piattaforme digitali (Google, Meta e TikTok) e presentare delle criticità e proposte per migliorare il benessere dei più giovani all'interno degli ambienti online. In quell' occasione sono emersi tre elementi principali:

1. la difficoltà, comune alla gran parte di ragazzi e ragazze, nel gestire il tempo all'interno delle piattaforme online e, in generale, di bilanciare in un equilibrio positivo le diverse attività quotidiane onlife;
2. i contenuti inadeguati, pericolosi, violenti, falsi, in grado di diminuire il benessere dei più giovani a volte condizionando lo stato d'animo e gli interessi;
3. il comportamento degli altri utenti della rete a volte incapaci di costruire relazioni adeguate all'interno delle piattaforme (es. i commenti sui social) ed in grado di impattare in modo negativo sul benessere digitale.

L'analisi compiuta dallo Youth Panel sul Digital Services Act sembra andare nella giusta direzione rispetto ad alcuni di questi elementi e ricalca, in parte, alcune richieste presentate alle piattaforme digitali Google, Meta e Tik Tok in occasione dell'incontro di settembre 2023.

#### CRITICITÀ EMERSE

Se, dunque gli elementi, anche più tecnici, possono trovare una nuova direzione con il DMA, nel confronto è emersa come ineludibile una formazione/sensibilizzazione adeguata, concreta ed efficace che si rivolga a tutta la comunità ed ai diversi contesti (non solo la scuola ad es.) per fornire maggiori strumenti per un benessere digitale che sia anche il risultato di approcci condivisi tra le Istituzioni.
Spesso i più giovani ma anche gli stessi adulti di riferimento e persino i docenti trovano difficoltà, ad esempio, nel comprendere ruolo e funzionamento degli algoritmi o quali possono essere gli effetti delle proprie azioni online, sia per sé stessi che per gli altri (come, ad esempio, i commenti sui social media). Come reperire dunque fonti attendibili e gestire i contenuti che vengono veicolati? Come gestire la propria identità digitale con una concreta ed efficace attenzione alla privacy ed alla sicurezza?

#### DOMANDE PER TUTTI GLI ATTORI ISTITUZIONALI

**Campagne di formazione/sensibilizzazione realizzate:**

- Quali campagne di sensibilizzazione avete realizzato ad oggi sui temi dell'online safety?
- Quali sono stati i temi e quali i target a cui vi siete rivolti?
- Che tipologia di strumenti avete utilizzato per i contenuti e per la loro diffusione?
- Dalla vostra valutazione quanto sono state efficaci o perché non hanno funzionato?
- Quali target non sono stati sino ad oggi oggetto delle vostre campagne?
- In merito alle nuove forme di tutela del DSA state progettando campagne specifiche?

#### PROPOSTA TRASVERSALE PER TUTTI GLI ATTORI ISTITUZIONALI

**Campagne di formazione/sensibilizzazione con il contributo dello Youth Panel**

È necessario che le campagne di sensibilizzazione rivolte a cittadini/e, ed in primis ai più giovani, siano in grado di fornire contenuti chiari ed espressione dei diversi elementi che permettono a ciascuno di vivere un positivo benessere digitale ed essere capace di un esercizio dei suoi diritti digitali.

**Per questo lo Youth Panel si offre di essere al vostro fianco, per la definizione di un piano straordinario di sensibilizzazione,** rivolto in primis ai più giovani, in cui ciascuna Istituzione sia coinvolta con i temi che sono parte della sua mission.
Tra dodici mesi, nel nostro prossimo incontro, speriamo di poter valutare insieme a voi alcune prime realizzazioni di questo piano e poterlo allargare a tutta la comunità.
Uno strumento possibile emersi nel confronto è quello di utilizzare le sale cinematografiche come momento di disseminazione per un uso sicuro e positivo della rete.

## CONCLUSIONI

Il presente rapporto documenta il lavoro svolto dallo Youth Panel del progetto Generazioni Connesse -SIC e le questioni emerse che costituiranno i punti focali della discussione, oltre alle proposte formulate, per le quali lo Youth Panel richiede un impegno concreto da parte delle istituzioni.

Le criticità individuate, le domande e le proposte sono state indirizzate sia a singoli attori istituzionali, in linea con le loro funzioni e mandati, sia a più attori quando le responsabilità sono condivise. Alcune proposte rimangono aperte e richiedono una riflessione collettiva da parte di tutti i partecipanti alla tavola rotonda.

Il monitoraggio del follow-up delle proposte avrà luogo a luglio 2025, in occasione della prossima edizione del Giffoni Film Festival, con l'obiettivo di verificare lo stato di avanzamento dei lavori e valutare i progressi compiuti dalle istituzioni in risposta alle raccomandazioni dello Youth Panel.

Questo incontro ha rappresentato un primo passo significativo verso la costruzione di un dialogo strutturato e continuativo tra lo Youth Panel del progetto Generazioni Connesse - SIC e le istituzioni, mirato a migliorare la sicurezza online e il benessere digitale dei più giovani. Il lavoro congiunto e le azioni concrete che ne deriveranno potranno contribuire a creare un ambiente digitale più sicuro e consapevole per tutti/e noi.