

Nova 2026. Parola all'Italia. Confronto deliberativo di sabato 27 giugno- Report tematici dei gruppi di discussione

Report del tema:

Tema 5 - Identità digitale, social media e tutela delle persone

Gruppo: 15

RESTITUZIONE

Il confronto ha affrontato in modo ampio e articolato il tema della sicurezza negli spazi digitali, evidenziando la complessità di bilanciare libertà, tutela degli utenti e responsabilità delle piattaforme. Il dibattito ha fatto emergere una pluralità di proposte, con un livello di difficoltà percepito elevato soprattutto per la natura tecnica e globale delle problematiche.

Domanda 1 – Quali priorità dovrebbe perseguire la politica per costruire uno spazio digitale più sicuro, libero e rispettoso dei diritti delle persone, con particolare riguardo per minori e donne?

Una prima linea di intervento riguarda il rafforzamento delle strutture di controllo e contrasto ai reati online. È stata più volte sottolineata la necessità di potenziare in modo significativo la polizia postale, a fronte dell'aumento e della diversificazione dei reati digitali, spesso mascherati attraverso profili falsi, truffe, ricatti e forme di estorsione.

Un altro punto centrale riguarda la tutela dei minori. Sono emerse proposte di restrizione dell'accesso ai social sotto una certa età (citando anche l'esempio di misure in discussione in altri Paesi europei come il limite ai 16 anni), insieme all'idea di sistemi di verifica più rigorosi in fase di registrazione. Tra le soluzioni proposte: controllo dell'intestazione delle SIM, verifica tramite SMS, utilizzo di identità digitali certificate (SPID o carta d'identità elettronica), fino all'ipotesi di sistemi europei integrati per l'autenticazione.

Accanto agli strumenti tecnici, è stato evidenziato il tema della responsabilità delle piattaforme digitali, con l'idea che debbano rispondere direttamente nel caso di mancata rimozione di contenuti segnalati o dannosi, soprattutto in presenza di violenza, hate speech o contenuti lesivi.

Molto forte anche il richiamo alla dimensione culturale ed educativa: la necessità di introdurre percorsi strutturati di educazione digitale nelle scuole, estesi anche agli adulti e alle famiglie, è stata considerata una condizione fondamentale. Secondo questa prospettiva, molti fenomeni problematici derivano da un uso non consapevole degli strumenti digitali più che dallo strumento in sé.

Infine, è emersa la consapevolezza che il problema non sia solo nazionale, ma globale: serve un coordinamento sovranazionale per affrontare i grandi attori del web e le dinamiche del cosiddetto lato

oscuro della rete (dark web, deep web, canali di comunicazione non controllati come alcune piattaforme di messaggistica).

Domanda 2 – Quali misure dovrebbero essere adottate per perseguire un controllo equilibrato dell'identità digitale, tutelando l'anonimato e al tempo stesso garantendo la responsabilità delle azioni da parte degli autori?

Sul tema dell'identità digitale il dibattito si è concentrato sul rapporto tra anonimato e tracciabilità. Una posizione emersa con forza sostiene la necessità di ridurre drasticamente l'anonimato online, introducendo sistemi di identificazione univoca e verificata per ogni utente, così da garantire responsabilità diretta delle azioni compiute in rete.

Sono state avanzate proposte di creazione di un'anagrafe digitale pubblica gestita da soggetti istituzionali, che attribuisca a ciascun cittadino un codice identificativo utilizzabile per l'accesso alle piattaforme. In questo modello, i social non riceverebbero dati personali completi, ma un identificativo certificato, utile a garantire autenticazione e tracciabilità.

Altre proposte includono sistemi di accesso multilivello (username, password e un terzo fattore di verifica), integrazione con documenti digitali europei e strumenti di sicurezza avanzati per ridurre abusi e falsificazioni.

Un ulteriore tema riguarda la governance dei dati: è stata espressa l'idea che le informazioni personali non debbano essere esclusiva proprietà dei privati, ma soggette a una forma di controllo pubblico o europeo, anche attraverso sistemi di backup istituzionali e strumenti di monitoraggio.

È stata inoltre sottolineata l'importanza di utilizzare sistemi di intelligenza artificiale per intercettare e segnalare rapidamente comportamenti dannosi (cyberbullismo, abusi, contenuti illegali), pur mantenendo la necessità di un intervento umano e istituzionale per la gestione dei casi.

Infine, è stato riconosciuto un nodo critico: l'effettiva applicabilità delle regole. L'esistenza di strumenti come VPN, numeri virtuali o canali alternativi di accesso rende difficile un controllo totale, evidenziando la necessità di agire non solo sulle piattaforme ma anche sulle infrastrutture e sui meccanismi che le circondano.

In sintesi, il confronto ha messo in luce una forte tensione tra sicurezza e libertà digitale, tra controllo e anonimato, evidenziando come la soluzione non possa essere univoca ma debba integrare strumenti tecnologici, norme europee, responsabilità delle piattaforme e soprattutto un investimento strutturale sull'educazione digitale e civica.