

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

Sintesi finale

I gruppi convergono su un'idea di fondo: lo spazio digitale va regolato come una piazza pubblica, bilanciando sicurezza, libertà e responsabilità, senza lasciare la gestione dell'identità online ai soli operatori privati; il nodo più controverso riguarda però lo statuto dell'anonimato, dove le posizioni divergono radicalmente, talvolta all'interno dello stesso gruppo.

Sull'età minima per l'accesso ai social la convergenza è molto ampia, anche se i valori indicati oscillano tra 14 e 16 anni; resta però una divergenza netta, con una tesi che considera il controllo dell'età un rischio di deriva repressiva della rete, da lasciare alla responsabilità delle famiglie, e un'altra che chiede invece una convergenza tra più agenzie educative. Non manca chi teme che qualunque divieto assoluto risulti aggirabile e controproducente, proponendo di puntare sull'educazione più che sul divieto.

Sul controllo dell'identità digitale prevale un modello di identificazione selettiva, capace di dimostrare requisiti come la maggiore età senza rivelare l'identità completa, spesso legato a strumenti come SPID, carta d'identità elettronica o portafoglio europeo di identità digitale. Una voce distinta si oppone con forza proprio a quest'ultimo strumento, temendo che accorpate tutti i dati della persona in un unico sistema centralizzato aumenti il monitoraggio indiscriminato, e propone invece sistemi decentralizzati con proprietà pubblica dei dati.

Il nodo più controverso di tutto il confronto riguarda l'anonimato: c'è chi sostiene che negli spazi pubblici digitali non debba essere considerato un diritto, chi lo vuole come regola generale con l'identificazione come sola eccezione soggetta a garanzie giudiziarie, chi lo ritiene addirittura inviolabile a tutela del dissenso politico. In un gruppo le due tesi opposte convivono senza che nessuna prevalga. Strettamente collegata è la richiesta, molto condivisa, che il controllo delle identità e la conservazione dei dati restino interamente pubblici, senza affidarsi a privati o a server stranieri; su questa linea si innesta anche una forte contrarietà a ogni forma di controllo generalizzato delle chat private, ritenuto sproporzionato perché chi agisce con dolo troverebbe comunque vie alternative, mentre verrebbero compressi i diritti di tutti.

Sull'educazione digitale la convergenza è pressoché unanime: materia curriculare stabile per studenti, famiglie e personale scolastico, affiancata da formazione delle forze dell'ordine e della magistratura sui reati digitali. Tra le proposte più originali, un'educazione che spieghi il funzionamento del "capitalismo della sorveglianza" per rendere i giovani consapevoli di come i loro dati vengono monetizzati, e un ritorno alle materie umanistiche — storia, filosofia, diritto — per restituire il senso critico che la sola alfabetizzazione tecnica non garantisce.

Sulla responsabilizzazione delle piattaforme convergono trasparenza sugli algoritmi, diritto a non essere profilati, tassazione dei profitti per finanziare educazione e ricerca pubblica, obblighi di rimozione rapida e presenza legale in Italia o in Europa; tra le misure più drastiche proposte, il blocco temporaneo di un'intera piattaforma a livello nazionale in caso di inadempienza grave. Strettamente legata è la richiesta di una sovranità digitale europea, con infrastrutture, cloud e piattaforme pubbliche alternative alle multinazionali, fino alla proposta di nazionalizzare le infrastrutture critiche.

Sulla tutela delle donne convergono sportelli pubblici dedicati e proposte normative più severe, come un reato specifico di deepfake sessuale non consensuale — anche se lo stesso gruppo che lo propone ne dubita l'efficacia pratica per la difficoltà di individuare gli autori — o, in una proposta più articolata, rendere il revenge porn perseguibile d'ufficio superando la querela di parte, ispirandosi a un modello che riconosce alle persone un vero diritto di proprietà sulla propria immagine. Sull'intelligenza artificiale converge l'obbligo di dichiarare i contenuti generati o manipolati, insieme al suo uso per filtrare contenuti offensivi, pur riconoscendo che i filtri automatici vengono spesso aggirati e restano insufficienti senza un controllo umano.

Chiudono il quadro alcune posizioni più isolate ma distintive: la richiesta di preservare sempre un contatto umano nei servizi digitalizzati, per non trasformare l'assistenza in pura dipendenza dagli strumenti informatici; un modello che limita l'intervento pubblico repressivo alle sole condotte gravissime e recidive, attraverso una sorta di "Daspo digitale" cautelare; una divergenza, interna a un gruppo, sul fatto che le istituzioni debbano abbandonare i social come canale ufficiale, contro chi osserva che per l'opposizione politica restano spesso l'unico strumento di visibilità; e un'analoga divergenza sui sistemi di reputazione online, capaci di limitare chi persevera in comportamenti scorretti ma temuti come strumento pericoloso se usati da un potere fuori controllo democratico. Trasversale a molti di questi temi resta infine la richiesta di un coordinamento europeo più efficace, sia per colmare il vuoto normativo sul diritto all'oblio sia per garantire alle forze dell'ordine un accesso più rapido ai dati delle piattaforme.

Questa sintesi è stata realizzata con il supporto dell'intelligenza artificiale partendo dai report redatti dai moderatori di ciascun tavolo di lavoro. Puoi trovare i report di ciascun tavolo a questo link:

<https://www.movimento5stelle.eu/nova/report20-27giugno>

Le proposte finali saranno invece elaborate senza l'utilizzo dell'intelligenza artificiale e utilizzando come fonte primaria i report dei singoli tavoli di lavoro, gli instant report degli eventi sul territorio, i contributi degli stakeholders tenendo anche conto dell'attività politica già svolta dal MoVimento 5 Stelle.