Oggetto: appello della Rete diritti umani digitali a rivedere la posizione italiana sul Child Sexual Abuse Regulation, in vista della votazione in seno al Consiglio dell'Unione europea.

Gentili,

Siamo a scrivervi a nome della Rete per i diritti umani digitali – la prima coalizione di organizzazioni della società civile italiana impegnate nella tutela dei diritti umani digitali – per chiedere formalmente al governo italiano di opporsi all'adozione del regolamento CSAR (Child Sexual Abuse Regulation), noto anche come "Chat Control", nelle competenti sedi europee.

Pur riconoscendo la piena legittimità e il valore dell'intento dichiarato dai promotori del provvedimento – ovvero quello di contrastare la diffusione e lo sfruttamento di CSAM (Child sexual abuse material) online – riteniamo che la proposta, tuttora in discussione presso il Consiglio dell'Unione europea, rappresenti una grave minaccia ai diritti fondamentali dei cittadini europei, in particolare al diritto alla riservatezza delle comunicazioni. Temiamo, inoltre, che essa possa introdurre un regime di sorveglianza di massa senza precedenti nel continente.

Se approvata, la proposta obbligherebbe i fornitori di servizi di comunicazione online (come WhatsApp, Telegram, Instagram, X/Twitter e altri) a garantire l'accesso indiscriminato alle conversazioni degli utenti, anche cifrate, qualora le autorità ne facciano richiesta. Basterebbe, infatti, il solo «rischio» che un servizio possa essere usato per scambiare CSAM (Child sexual abuse material) per prevedere l'obbligo di incorporare un sistema di scansione automatica di tutti i contenuti.

La possibilità che tale scenario si concretizzi sta suscitando forti preoccupazioni nella cittadinanza e rischia di incrinare la fiducia nelle istituzioni.

Introdurre uno strumento di scansione preventiva significherebbe, ai fatti, trattare *a priori* ogni cittadino come un potenziale criminale, invertendo la logica dello Stato di diritto. La scansione – definita *client-side scanning* – avverrebbe direttamente sul dispositivo personale dell'utente (lato *client*), aggirando addirittura la crittografia *end-to-end*, che oggi protegge milioni di persone, inclusi giornalisti, attivisti, avvocati, magistrati, testimoni di giustizia, medici.

Approvare "Chat Control" aprirebbe una *backdoor*, una "porta sul retro", per spiare ogni conversazione privata: la cifratura non sarebbe più realmente *end-to-end*, poiché uno degli "end" (il dispositivo stesso) diventerebbe parte attiva del controllo e a quel punto non solo le forze dell'ordine, ma anche hacker e truffatori, sarebbero facilitati nell'intercettare comunicazioni private o professionali, che diverrebbero intrinsecamente vulnerabili.

La tutela dei minori non può diventare un pretesto per implementare una sorveglianza di massa. Se l'obiettivo è davvero quello di rafforzare la protezione dei minori, riteniamo che gli sforzi debbano concentrarsi sull'aumento delle risorse investigative, sulla rimozione tempestiva dei contenuti illeciti e sul sostegno alle vittime; e non sull'adozione di scanner universali e database centralizzati di "indicatori" gestiti dalle forze dell'ordine, che comportano il rischio concreto di violazioni sistematiche dei diritti fondamentali.

Nel 2023 il Parlamento europeo aveva già tracciato una linea chiara: no allo *scanning* indiscriminato, se non in presenza di sospetto concreto. Vi chiediamo dunque di ribadire quella linea, non solo perché è giusto, ma anche perché è la scelta politicamente più solida. **Difendere la privacy è nel vostro interesse: ogni tentativo di controllo generalizzato mina la fiducia dei cittadini nelle istituzioni democratiche.**

L'Italia non sarebbe certo sola nel respingere la proposta, ma si unirebbe a diversi Stati membri, tra cui Austria, Belgio, Repubblica Ceca, Finlandia, Paesi Bassi, Polonia, Lussemburgo e - da ultima - Germania. Dunque, votare contro "Chat Control" significherebbe far parte di un fronte che difende diritti digitali, privacy, integrità della crittografia e Stato di diritto - principi oggi più che mai sotto i riflettori, in Europa.

Numerose analisi indipendenti – tra cui quelle di Internet Society ed Electronic Frontier Foundation – hanno evidenziato che non esiste alcun modo per conciliare la crittografia end-to-end (E2EE) con un obbligo di scansione automatica e continua dei contenuti. La stessa Commissione europea ha ammesso che i *detection orders* andrebbero considerati solo come "extrema ratio", persino nei casi che coinvolgono comunicazioni cifrate, mentre le principali autorità europee in materia di protezione dei dati (EDPB e EDPS) hanno ricordato che l'applicazione di misure generali e indiscriminate violano i principi di necessità e proporzionalità sanciti dalla normativa Ue.

Inoltre, la giurisprudenza europea ha già più volte bocciato approcci simili, come nel caso della conservazione indiscriminata dei dati o della sorveglianza generalizzata, e accademici, esperti e organizzazioni della società civile attive nella difesa dei diritti digitali - tra cui European Digital Rights (EDRi), Access Now, La Quadrature du Net e molte altre - hanno espresso posizioni simili.

Alla luce di quanto richiamato fin qui, siamo dunque a chiedere al governo italiano di opporsi all'implementazione di un sistema di sorveglianza di massa come "Chat Control" in seno al Consiglio dell'Unione europea e di adottare misure concrete volte a difendere i cittadini e le cittadine italiane, a proteggere le loro libertà fondamentali e a garantire l'integrità delle comunicazioni.

Di fronte a una minaccia pericolosa e sproporzionata come quella che costituisce la proposta CSAR/Chat Control, riteniamo che il governo italiano debba assumere una posizione chiara, a tutela della democrazia e della propria popolazione, e fare pressioni affinché vengano presi in considerazione altri strumenti che non prevedano un abuso sistematico nei confronti di tutte e tutti, in nome del contrasto ad altri reati.

Ringraziando sin d'ora per l'attenzione che si vorrà rivolgere alle nostre richieste, restiamo a disposizione per fornire ogni ulteriore contributo e chiarimento sul tema.

Distinti saluti

Rete diritti umani digitali

The Good Lobby
Privacy Network
StraLi
Period Think Tank
Hermes Center
Amnesty International Italia