

Chat Control: la Danimarca riscrive la norma, ma i problemi sulla privacy rimangono

Dopo il mancato accordo tra i 27 Stati membri e il conseguente rinvio del voto, il "[Chat Control](#)" è tornato al centro dell'**agenda digitale europea**. Giovedì 30 ottobre la presidenza danese del Consiglio dell'Unione europea ha riaperto il dossier più controverso della legislatura, diffondendo un documento di discussione che riscrive la proposta di regolamento CSAR (*Child Sexual Abuse Regulation*). Il testo, nato per combattere la diffusione online di **materiale pedopornografico**, puntava a imporre alle piattaforme digitali l'obbligo di **sorvegliare in modo automatico** i messaggi privati, anche quelli cifrati end-to-end, portando a uno **screening preventivo** dei contenuti (audio, foto, video). La nuova bozza segna un'inversione di rotta: i controlli non sarebbero più imposti in maniera indiscriminata, ma lasciati alla **discrezionalità dei singoli fornitori** di servizi, introducendo una "facoltatività" che mira a salvare la norma dopo il naufragio del voto in seguito al veto della Germania.

Si tratta di una mossa che tenta di ricucire la spaccatura politica sull'equilibrio, sempre più fragile, tra tutela dei minori e diritto alla privacy. Il 9 ottobre 2025 il Consiglio dell'Unione europea aveva annunciato il **rinvio del voto** sulla norma. Non si era raggiunta la maggioranza qualificata necessaria e la proposta era rimasta sospesa a tempo indefinito. La **Germania** aveva guidato il fronte del "no". Insieme a Berlino si erano schierati anche Austria, Olanda, Finlandia, Polonia e Repubblica Ceca, mentre altri Paesi, incerti o divisi al loro interno, avevano preferito non esporsi. Il [Chat Control](#), nella sua formulazione iniziale, elaborata nel 2022, prevedeva l'obbligo per le piattaforme digitali di scansionare automaticamente i messaggi privati attraverso algoritmi e sistemi di intelligenza artificiale in grado di individuare immagini, testi o video riconducibili ad abusi sessuali su minori. Una misura pensata per contrastare un fenomeno grave e dilagante, ma giudicata da molti governi e associazioni come una minaccia diretta alla riservatezza delle comunicazioni. Le obiezioni si concentrano su due punti cruciali: la possibile compromissione della cifratura e il rischio di instaurare una **sorveglianza di massa**. Gli esperti di sicurezza avvertono che l'apertura di "backdoor" per consentire la scansione dei contenuti cifrati renderebbe **vulnerabile l'intero ecosistema digitale**, esponendo gli utenti a intrusioni e abusi. Un simile sistema porterebbe a un **controllo di massa**, con una quantità altissima di falsi positivi e il rischio di criminalizzare conversazioni innocue e inciderebbe direttamente sulla libertà di stampa e sulla protezione delle fonti giornalistiche, oltre che sulla sicurezza di attivisti e whistleblower.

La presidenza danese sta ora cercando un **compromesso** che ammorbidisca la norma, salvi la legge e, al tempo stesso, preservi la fiducia dei cittadini in un'Europa che rischia di diventare il **laboratorio della sorveglianza digitale**. La revisione danese, pur attenuando l'obbligatorietà della scansione, non ne elimina le criticità: spostata semplicemente il

Chat Control: la Danimarca riscrive la norma, ma i problemi sulla privacy rimangono

baricentro del controllo dallo Stato alle piattaforme tecnologiche, delegando loro una funzione di **vigilanza privata** che sfugge a ogni reale controllo democratico. Il futuro del Chat Control rimane così incerto. Il Parlamento europeo ha già indicato la preferenza per un sistema di monitoraggio mirato, autorizzato da un giudice e non basato su controlli automatici. Se la nuova bozza dovesse essere approvata, si aprirebbe un precedente destinato a incidere sull'intero quadro normativo europeo in materia di **privacy digitale**. La **logica preventiva**, applicata oggi alle chat, potrebbe domani estendersi ad altri ambiti, dal contrasto al terrorismo al controllo dell'informazione. In gioco non c'è solo una legge: c'è l'idea stessa di cittadinanza digitale. Accettare la scansione dei messaggi invocando la scusa di un bene superiore, anche se su **base volontaria**, significherebbe introdurre una forma di sorveglianza permanente, un **super-Panopticon elettronico** in nome della sicurezza.



Enrica Perucchiatti

Laureata con lode in Filosofia, vive e lavora a Torino come giornalista, scrittrice ed editor.

Collabora con diverse testate e canali di informazione indipendente. È autrice di numerosi saggi di successo. Per *L'Indipendente* cura la rubrica Anti fakenews.