Il regolamento sul cosiddetto "EU Chat Control" è arrivato a una fase decisiva: l'UE si prepara a votare una norma che imporrebbe alle piattaforme di messaggistica di installare algoritmi capaci di scansionare messaggi, immagini e file privati, anche cifrati end-to-end, per scandagliare messaggi, immagini, video, note vocali alla ricerca di abusi sessuali su minori. Presentata come una misura necessaria per proteggere i bambini online, l'iniziativa comporterebbe, però, un **controllo preventivo e generalizzato delle comunicazioni private**. Non si tratterebbe, infatti, di indagini mirate, ma di una sorveglianza estesa a ogni cittadino, con il rischio di errori, falsi positivi e intrusioni indebite. Le istituzioni europee giustificano il progetto con l'aumento dei casi di pedofilia, pedopornografia e adescamento di minori, fenomeni in crescita in diversi Stati membri, soprattutto tra adolescenti. Esperti e attivisti avvertono, invece, che forzare la cifratura esporrebbe milioni di utenti a **vulnerabilità** sfruttabili non solo dalle autorità, ma anche da hacker e criminali informatici. Il pericolo è che le chat private vengano trasformate in spazi sorvegliati per definizione, dove la promessa di sicurezza si traduce in **sorveglianza di massa** e in un indebolimento sostanziale dei diritti fondamentali. Se approvato, il regolamento creerebbe un obbligo per le piattaforme, compreso il caricamento di contenuti sospetti su database centralizzati per confronti con materiale illecito.

Sul piano politico, il campo si sta dividendo con chiarezza, senza che vi sia ancora una maggioranza certa. Allo stato attuale, oltre la metà dei Paesi appoggia la proposta, avanzata per la prima volta nel maggio 2022 dall'allora Commissaria UE per gli Affari interni, Ylva Johansson. Attualmente, **15 Stati** sostengono la proposta, **8 Stati** si oppongono ufficialmente, e **4 sono indecisi**, come riporta la piattaforma online Fightchatcontrol.eu. Tra quelli **contrari** ci sono Austria, Belgio, Germania, Lussemburgo, Repubblica Ceca, Finlandia, Paesi Bassi e Polonia. Dopo alcune titubanze, il governo tedesco guidato dal cancelliere Merz ha confermato l'opposizione espressa con forza dal precedente esecutivo Spd-Verdi-Liberali. Nei Paesi contrari emerge una crescente consapevolezza tecnica: si avverte che l'introduzione di meccanismi di scansione preventiva comprometterebbe gli standard di sicurezza, trasformando la cifratura end-to-end in un guscio fragile. Le backdoor o i bypass necessari per consentire i controlli aprirebbero inevitabilmente varchi a intrusioni, abusi e attacchi da parte di soggetti malintenzionati. **Tra i sostenitori figurano Italia, Francia e Spagna**. Gli indecisi comprendono Estonia, Grecia, Romania e Slovenia. Nel Parlamento Europeo la difficoltà non è solo nazionale, ma parlamentare: critiche arrivano da gruppi che normalmente non si schierano insieme – Verdi, Alleanza Libera Europea, parte dei social-liberali, alcuni eurodeputati identitari o "populisti" – tutti accomunati dalla convinzione che «proteggere i bambini online è possibile senza una sorveglianza di massa». Sul fronte dei conservatori, anche l'europarlamentare finlandese del Partito Popolare Europeo (Ppe), Aura Salla, ha affermato che il regolamento «pone un

rischio enorme di esporre le nostre comunicazioni e foto private». Le opposizioni non negano la gravità del fenomeno degli abusi su minori, ma rifiutano che la risposta debba passare necessariamente attraverso un controllo generalizzato e obbligatorio delle comunicazioni private. Secondo uno studio disposto dal Parlamento Europeo e presentato alla Commissione su Libertà Civili, Giustizia e Affari Interni, il regolamento rischia, infatti, di avere un impatto negativo per l'**elevato tasso di errore** sul rilevamento degli abusi nei messaggi e nei file, a partire dai contenuti diffusi dagli utenti in modo consensuale.

Alla soglia del voto, la questione non è più soltanto tecnica, ma politica e culturale: se approvata, la norma introdurrebbe per la prima volta un sistema di controllo preventivo e obbligatorio sulle comunicazioni private. L'impatto sarebbe dirompente: ogni messaggio, anche tra cittadini privi di qualsiasi sospetto, verrebbe sottoposto a un **filtro algoritmico**, svuotando il principio stesso della riservatezza sancito dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'UE. Dal punto di vista della sicurezza, l'imposizione di backdoor o sistemi di scansione all'interno delle piattaforme cifrate aprirebbe **vulnerabilità** che potrebbero essere sfruttate non solo dalle autorità, ma anche da hacker, criminali e potenze straniere. Il **monitoraggio generalizzato** produrrebbe, inoltre, una mole enorme di dati sensibili da gestire e archiviare, con il rischio di abusi, fughe di informazioni e perdita di controllo da parte degli utenti. La fallibilità degli algoritmi non è un dettaglio tecnico: **falsi positivi** potrebbero portare a segnalazioni ingiuste (come già avviene con la "polizia predittiva"), criminalizzando conversazioni private, immagini innocue o scambi professionali tutelati dal segreto medico, legale o giornalistico. Un simile contesto favorirebbe l'autocensura e inciderebbe sulla libertà d'espressione, trasformando il diritto a comunicare in un'attività sottoposta a **sorveglianza preventiva**. A queste criticità si aggiunge il rischio politico: un regolamento percepito come invasivo eroderebbe la fiducia dei cittadini nelle istituzioni europee, aprendo la strada a un modello di sospetto generalizzato. Anche sul piano economico, gli operatori tecnologici si troverebbero a fronteggiare costi elevati, nuovi rischi legali e una concorrenza alterata. Senza un controllo parlamentare stringente, trasparenza assoluta e tutela effettiva della crittografia, il regolamento rischia di trasformarsi in un apparato di sorveglianza istituzionalizzato, più che in uno strumento di protezione. Dall'11 settembre a oggi, in nome della sicurezza, si stanno erodendo privacy e diritti fondamentali, legittimando norme draconiane e imponendo misure liberticide. Al di là della retorica, non tutto ciò che promette protezione garantisce sicurezza, e **non tutto ciò che proclama sicurezza tutela davvero la libertà**.

La legge europea sul Chat Control è a un punto di svolta

Enrica Perucchietti

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.