

I rischi reali della normativa "Chat Control"

Il Parlamento Europeo ha riconfermato Chat Control, la deroga che consente la scansione volontaria dei messaggi privati. Ne parliamo con Stefano Epifani, presidente della Fondazione per la Sostenibilità Digitale, tra dubbi sull'efficacia e rischi per la privacy

di Walter Ferri

A inizio mese, il Parlamento Europeo ha riconfermato Chat Control, la controversa deroga temporanea alla direttiva ePrivacy che consente alle aziende di scandagliare, su base volontaria, i messaggi privati degli utenti alla ricerca di materiale pedopornografico. Diversi esperti mettono in dubbio che questa erosione dei diritti digitali sia realmente efficace rispetto agli obiettivi dichiarati e persino molti esponenti della classe politica si sono detti contrari a questa direzione. Ciononostante le istituzioni europee premono con decisione perché la deroga venga mantenuta. Per fare chiarezza sulla questione, abbiamo raggiunto Stefano Epifani, presidente della Fondazione per la Sostenibilità Digitale, ente che si pone l'obiettivo di promuovere

re la trasformazione digitale, ma con un approccio orientato alla sostenibilità.

Recentemente il Parlamento Europeo ha votato sulla reintroduzione del cosiddetto "Chat Control 1.0", in condizioni che di fatto hanno favorito l'approvazione della mozione, applicando meccanismi procedurali che sono stati definiti da alcuni come antidemocratici. Quanto è regolare l'iter che è stato adottato?

Formalmente, tutto regolare. Sostanzialmente, no. Il Parlamento aveva respinto il rinnovo il 26 marzo, 311 voti contro 228, e la deroga era scaduta il 3 aprile. Doveva finire lì. Invece il 2 luglio il Consiglio ha ripresentato un nuovo testo con effetti sostanzialmente equivalenti, utilizzando una diversa base giuridica anziché una proroga tecnica dell'atto ormai scaduto. E la seconda lettura ribalta l'aritmetica: per fermare la proroga serve la maggioranza assoluta, 361 voti su 720, nell'ambito della procedura adottata, con il voto fissato al 9 luglio, ultimo giorno prima delle ferie, ad aula mezza vuota. Procedura d'urgenza, senza il passaggio in commissione. Se una procedura serve a neutralizzare un voto già espresso, il problema non è la legalità o la coerenza formale, ma la legittimazione. E un'Unione che vince ai supplementari procedurali ciò che ha perso nel merito si sta facendo male da sola.

Al momento stiamo parlando di Chat Control 1.0, ma le istituzioni stanno già lavorando al suo successore, Chat Control 2.0. Quali sono le principali differenze tra i due regolamenti?

Sono due oggetti diversi, e confonderli fa comodo a chi li propone. Quello votato il 9 luglio è il regime temporaneo: proroga fino ad aprile 2028 della facoltà, per i fornitori,

di scansionare volontariamente le comunicazioni cercando materiale di abuso e adescamento, senza imporre la scansione delle comunicazioni cifrate end-to-end. Il secondo procedimento è il regolamento permanente proposto dalla Commissione nel 2022: valutazioni del rischio, misure di prevenzione, ordini di rimozione e blocco, un Centro europeo dedicato; e il Consiglio, nella posizione di novembre 2025, propone di rendere stabile la possibilità di controllo. Insomma: l'1.0 concede un permesso a termine, il 2.0 costruisce l'infrastruttura definitiva. Il primo è la deroga. Il secondo è l'architettura.

Le aziende non sono obbligate a scansionare i messaggi degli utenti, tuttavia le misure previste dalla versione definitiva di Chat Control delineano un ecosistema in cui vengono comunque gravate da numerose responsabilità. Siamo ancora nella sfera della volontarietà, o le società saranno di fatto costrette, per via indiretta, a scandagliare i messaggi delle persone?

Un comportamento è volontario quando l'ordinamento è realmente indifferente al suo esito. Formalmente, nessuna norma impone ai fornitori di effettuare la scansione. Ma il quadro regolatorio complessivo rende quella scelta economicamente, reputazionalmente e operativamente più conveniente rispetto al non farla. Per questo la volontarietà è discutibile sul piano sostanziale. Nella contrattualistica lo vediamo ogni giorno: la clausola "facoltativa" il cui rifiuto costa più dell'adesione si chiama, con un termine tecnico, condizionamento. Certo, nessuna norma dice "devi". Ma il diritto non si legge soltanto per enunciati: si legge anche per incentivi. E un sistema che rende la sorveglianza la soluzione meno onerosa finirà inevitabilmente per produrre sorveglianza, con il vantaggio, per il legislatore, di poter dire che l'hanno scelta le aziende. Sen-

za considerare, e questo è dirimente, che la volontarietà è delle piattaforme, non degli utenti.

La motivazione dichiarata di una simile misura è quella di tutelare i minori, arginare la diffusione di materiale pedopornografico e prevenire l'adescamento online. Ammesso e non concesso che si sia disposti a mettere da parte la privacy in favore di questi intenti, Chat Control è una strategia efficace per raggiungere i risultati prefissati?

Le prove disponibili non dimostrano che la scansione generalizzata sia uno strumento particolarmente efficace contro le reti criminali più organizzate. Chi produce e scambia quel materiale ha una caratteristica che il legislatore finge di ignorare: si adatta. Migra verso piattaforme non cooperative, verso canali cifrati fuori giurisdizione, verso il darknet. La scansione di massa, per costruzione, guarda dove i criminali organizzati non stanno: nelle chat di miliardi di persone comuni. Con quali risultati? Montagne di falsi positivi da smaltire, forze investigative sommerse di segnalazioni inutili, risorse sottratte alle indagini mirate che funzionano davvero. È come svuotare il mare con un colino e rivendicare il merito delle alghe rimaste sul fondo. La protezione dei minori merita strumenti seri: indagini sotto copertura, cooperazione internazionale, prevenzione. Merita, in ultima analisi, di non essere usata come argomento che chiude ogni discussione invece di aprirla.

Sempre sulla tutela dei minori, parallelamente a Chat Control, si sta parlando molto del divieto di accesso a social e siti pornografici per i giovani, misura che imporrebbe

di fatto controlli anagrafici a tutti coloro che navigano in rete. Considerando che anche quest'altra soluzione viene spesso considerata inefficace, cosa possiamo dire a coloro che temono che queste norme siano dei pretesti per imporre, per vie traverse, un capillare sistema di sorveglianza digitale?

Che il timore è fondato, e che negarlo sarebbe disonesto. Molte infrastrutture di identificazione costruite per uno scopo finiscono per trovarne altri: la storia della sorveglianza è anche la storia degli scopi che cambiano. Nasce per il terrorismo, si applica ai reati comuni. Nasce per i minori, si estende ai "troll", come si discute in Australia. Non serve imma-

Il timore che queste norme siano dei pretesti per imporre un capillare sistema di sorveglianza digitale è fondato, e negarlo sarebbe disonesto

ginare governi malvagi: basta osservare che le architetture sopravvivono ai contesti che le hanno giustificate. E qui sta il punto di metodo. La domanda da porre a ogni strumento di questo tipo non è "ci fidiamo di chi lo

userà oggi?", ma "questa architettura resta innocua in mano a chi non merita fiducia?". Se la risposta è no, lo strumento non va costruito. Perché i dati si cancellano, le leggi si abrogano. Le infrastrutture, invece, restano. ■

Walter Ferri



Per *L'Indipendente* si occupa di analisi nel campo della tecnologia, dei diritti informatici, della privacy e dei nuovi media, indagando le implicazioni sociali ed etiche delle nuove tecnologie. È coautore e curatore del libro *Sopravvivere nell'era dell'Intelligenza Artificiale*.