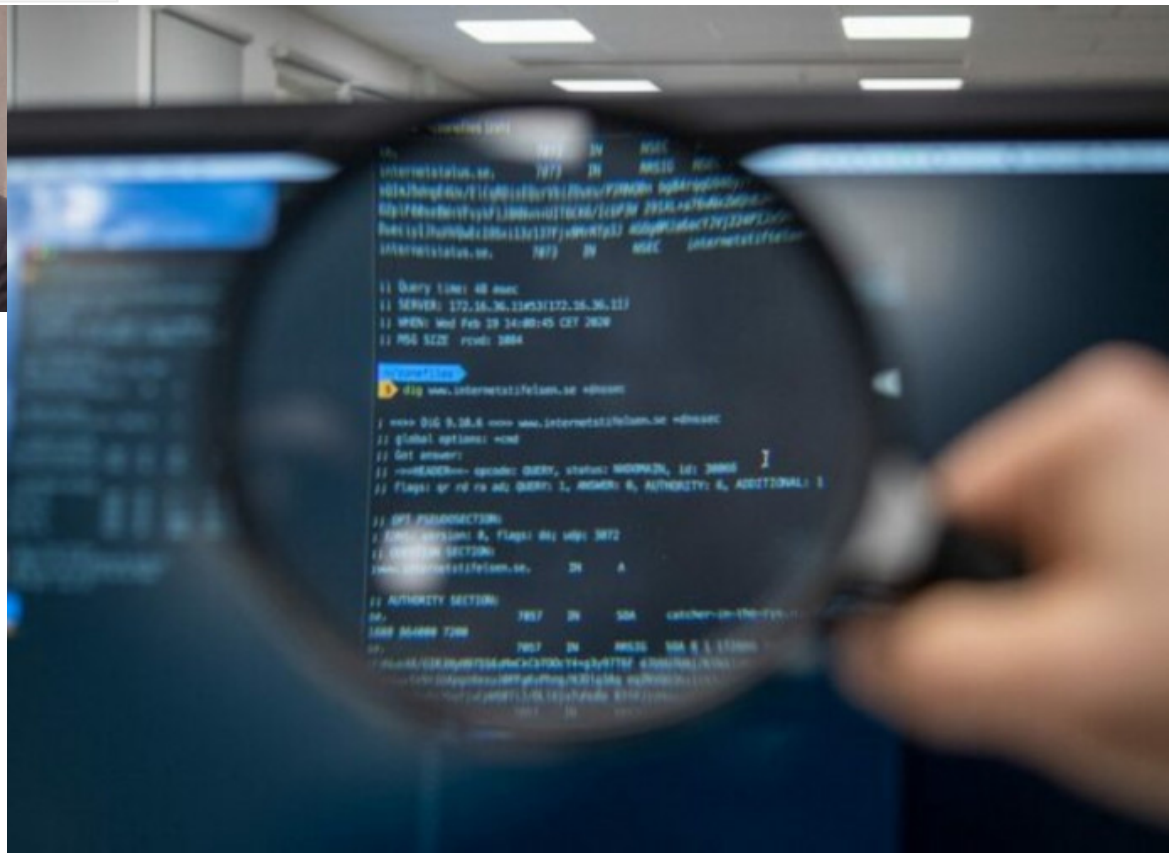
LA NUOVA BUSSOLA QUOTIDIANA
Direttore Riccardo Cascioli
FATTI PER LA VERITÀ

GRANDE FRATELLO

Chat Control, un sistema di sorveglianza di massa

EDITORIALI 15_07_2026

Maurizio Milano



Quasi invisibile al grande pubblico, si è consumata una partita decisiva sulla privacy: la proroga del regime “Chat Control 1.0”, che permette alle piattaforme digitali di scansionare i messaggi privati dei cittadini alla ricerca di materiale pedopornografico. Alla base c’è il Regolamento (UE) 2021/1232, una deroga temporanea alla direttiva ePrivacy pensata per consentire ai grandi provider di usare sistemi algoritmici

automatizzati per individuare il cosiddetto Child Sexual Abuse Material (CSAM). Questa deroga doveva scadere il 3 aprile 2026, in attesa di un nuovo quadro permanente (Chat Control 2.0), ma i negoziati su quest'ultimo si sono fermati per l'opposizione di crittografi, attivisti e alcuni governi nazionali, preoccupati per l'impatto sui diritti fondamentali.

Il 26 marzo il Parlamento europeo vota sulla proroga di Chat Control 1.0: 307 deputati votano contro l'estensione, 306 a favore, 24 si astengono. Per un solo voto, la scansione di massa viene bocciata. Passa anche un emendamento che imporrebbe di restringere il perimetro a singoli utenti o gruppi già sospettati su ordine di un'autorità giudiziaria, per impedire un accesso indiscriminato alla corrispondenza di milioni di comunicazioni private. Con la scadenza della proroga, le grandi piattaforme sospendono le scansioni in Europa; nel giro di poche settimane, tuttavia, l'apparato istituzionale si riorganizza per ribaltare l'esito politico.

Il 2 luglio il Consiglio dell'Unione Europea decide infatti di adottare come propria la proposta originaria della Commissione – cioè la versione appena bocciata dall'aula – facendola diventare "posizione del Consiglio" e attivando così la procedura di seconda lettura. Le regole del Parlamento stabiliscono che per respingere o emendare la posizione del Consiglio non basta la maggioranza dei presenti, ma occorre la maggioranza assoluta di tutti i 720 deputati, cioè 361 voti. Il tabellone delle votazioni del 9 luglio registra 314 voti contrari, 276 favorevoli, 17 astenuti. La maggioranza dei votanti ha nuovamente bocciato l'estensione, ma non ha raggiunto la soglia formale: la legge passa prorogando Chat Control 1.0 fino al 3 aprile 2028. Un'infrastruttura di sorveglianza respinta per ben due volte rientra così attraverso le pieghe procedurali, grazie a regole che trasformano un voto contrario in una mancata opposizione efficace. A che cosa serve il Parlamento Europeo? Qual è il livello effettivo di democrazia delle nostre istituzioni?

"Protect children, not predators": così il presidente del Partito Popolare Europeo, Manfred Weber, alla vigilia del voto aveva riassunto su X la posta in gioco. Chi contesta la misura, secondo lo slogan, non vuole "proteggere i bambini" e li lascia in balìa dei "predatori". Nessuno nega, ovviamente, l'urgenza di combattere la pedopornografia online, ma ciò va contemperato con la tutela del diritto alla privacy e con esigenze di proporzionalità. La preoccupazione è che una volta creato un apparato tecnico capace di scandagliare in massa messaggi e allegati, il confine tra lotta al crimine e sorveglianza strutturale dei cittadini diventi estremamente sottile. La vera questione, per il cittadino europeo, non è quindi se "difendere i minori", ma quali strumenti stiamo

accettando e con quali controlli democratici di tutela.

Dopo il 9 luglio, molti comunicati stampa parlano di "vittoria a metà": Chat Control 1.0 viene prorogato, ma le app con crittografia end-to-end, come WhatsApp, Signal e iMessage, sono escluse dal perimetro della scansione. Rimangono esposte alla scansione "volontaria", ma fortemente incentivata, email come Gmail e iCloud, messaggistica diretta non cifrata su Instagram e Facebook e archivi cloud dove la protezione è lato server. Prima della sospensione di aprile 2026, l'ecosistema Meta da solo generava la quasi totalità delle segnalazioni inviate alle forze dell'ordine europee, esaminando centinaia di migliaia di chat ogni anno. Anche se la crittografia per il momento è salva, rimane il fatto che la maggioranza delle comunicazioni digitali europee resta sotto un regime orwelliano che normalizza la scansione automatizzata alla ricerca di contenuti sospetti.

Il controllo algoritmico è estremamente invasivo e lesivo della privacy, ma almeno è efficace? I dati ufficiali della Polizia criminale federale tedesca indicano che circa il 48% delle segnalazioni automatizzate risulta essere un "falso positivo" o comunque penalmente irrilevante. Le statistiche svizzere, in un contesto diverso ma collegato alle stesse reti, parlano di tassi di falsi positivi fino all'80%. In termini concreti, quasi la metà (o più) delle comunicazioni private segnalate coinvolge cittadini innocenti, vittime solo di un algoritmo di analisi automatizzata che scambia per materiale illecito foto di famiglia, meme, o scambi di immagini intime tra adolescenti. Tanto rumore per nulla?

No, peggio ancora perché le forze dell'ordine si trovano sommerse da migliaia di allarmi inutili, distogliendo tempo e risorse dalle indagini mirate sulle reti criminali del dark web, che continuano invece a richiedere strumenti investigativi tradizionali e operazioni di intelligence mirate. La stessa Commissione europea riconosce che la scansione di massa rappresenta solo una parte delle segnalazioni complessive, mentre la maggioranza dei casi deriva da denunce specifiche, monitoraggio di contenuti pubblici e azioni di polizia focalizzate.

Si sta davvero costruendo un sistema più efficace per proteggere i minori? Oppure si è iniziato a creare una "architettura della sorveglianza" generalizzata che contraddice al principio fondamentale e costituzionalmente garantito della segretezza delle comunicazioni? Il vero banco di prova sarà il regolamento "Chat Control 2.0", che potrebbe configurarsi come un sistema permanente di scansione generalizzata e obbligatoria. Per superare la barriera della crittografia, la proposta include il cosiddetto client-side scanning: l'algoritmo si installa direttamente sul telefono o sul computer

dell’utente e analizza i contenuti prima che siano cifrati.

Più di 400 accademici hanno avvertito che questo modello crea una capacità di sorveglianza senza precedenti e nuove vulnerabilità. Con un semplice aggiornamento del software il controllo preventivo potrebbe essere esteso al contrasto della cosiddetta “misinformation” e “disinformation”, con la possibilità di bloccare sul nascere opinioni ritenute “estremiste” o comunque non gradite all’establishment. L’impressione è che si prosegua con la solita “cultura dell’emergenza”: si parte da istanze reali ma che poi vengono strumentalizzate ed utilizzate come leva politica per ottenere ben altri obiettivi rispetto a quelli dichiarati.

In conclusione: vogliamo davvero consegnare alle istituzioni e a fornitori privati un dispositivo che normalizza la sorveglianza preventiva delle nostre comunicazioni personali? Vogliamo davvero accettare come “nuova normalità” un livello strutturale di sospetto automatizzato? Chi tace, purtroppo, acconsente.