



ProVita
& Famiglia

CHAT CONTROL

No al controllo di massa
nei nostri cellulari



Cos'è il Chat Control

Ogni giorno scambi messaggi, foto e documenti con familiari, amici, colleghi. **Lo fai dando per scontato che nessuno li legga al di fuori del destinatario.** L'Unione Europea ha proposto un Regolamento che cancellerebbe questa fondamentale garanzia di privacy.

Lo chiamano "Regolamento per la prevenzione e il contrasto degli abusi sessuali sui minori" (CSAR), ma **il contenuto non corrisponde** a questo scopo più che condivisibile. Lo scopo fondamentale del progetto — ed è il motivo per cui viene chiamato **"Chat Control"** — è quello di autorizzare e addirittura obbligare le piattaforme di comunicazione (come Google, Meta, Telegram, Microsoft) a **scansionare automaticamente i messaggi privati** di tutti gli utenti, prima che siano inviati.

Il meccanismo è semplice. La Commissione Europea o un'autorità nazionale può emettere un **"ordine di rilevamento"** (detection order) nei confronti di un'azienda. L'azienda è allora obbligata a installare un **filtro automatico** che analizza il contenuto di ogni messaggio — testo, immagini, video, audio — prima dell'invio o alla ricezione. L'utente non viene informato né della scansione né dell'eventuale segnalazione.

Il pretesto dichiarato è il contrasto alla pedopornografia online. Uno scopo nobile e fondamentale. Ma il materiale pedopornografico circola prevalentemente su reti chiuse, canali anonimi e server dedicati — non sulle chat ordinarie tra cittadini. Gli stessi esperti di sicurezza informatica e le forze dell'ordine riconoscono che **la scansione indiscriminata di massa non raggiunge i criminali organizzati e produce un volume enorme di segnalazioni errate** a carico di cittadini innocenti. La segnalazione massiccia di "falsi positivi", paradossalmente, ingolfa e complica proprio il lavoro degli investigatori.

CHAT CONTROL 1.0 E CHAT CONTROL 2.0

Il Chat Control esiste in due versioni. La prima — "Chat Control 1.0" — è una deroga temporanea alla direttiva ePrivacy che consente (ma non obbliga) le aziende a scansionare le comunicazioni non protette da crittografia end-to-end. È già in vigore.

La seconda — il "Chat Control 2.0", ovvero il Regolamento CSAR — è la proposta di renderlo **obbligatorio e permanente**. Prevede ordini di rilevamento vincolanti, la scansione anche dei canali crittografati E2E come WhatsApp e Signal (tramite il "client-side scanning"), la verifica dell'età degli utenti e la creazione di un **"centro europeo di controllo"**.

	CHAT CONTROL 1.0	CHAT CONTROL 2.0 (CSAR)
Natura	Deroga temporanea	Regolamento permanente
Obbligo per le aziende	Facoltativo	Obbligatorio
Canali E2E (WhatsApp, Signal)	Esclusi	Inclusi (client-side scanning)
Durata	Con scadenza	Senza scadenza

Nota: le chat ordinarie di Telegram non sono crittografate end-to-end e rientrano già nel perimetro del Chat Control 1.0. Solo le "chat segrete" di Telegram sono protette dalla crittografia.

Perché ti riguarda

La propaganda istituzionale dell'UE presenta il Chat Control come uno strumento indispensabile contro i predatori di minori online. Ma le **implicazioni pratiche** vanno molto oltre questo condivisibile scopo. Per cercare contenuti illegali mettono sotto sorveglianza diretta le comunicazioni di tutti i cittadini: una sproporzione del tutto incostituzionale.

È come se le poste fossero obbligate ad aprire e leggere tutte le nostre comunicazioni private, prima di consegnarle al destinatario, per verificare eventuali contenuti illegali. **Un approccio tipico degli stati totalitari.**

Il Regolamento sul Chat Control implica soprattutto tre grandi rischi.

01

UN ALGORITMO RIPROGRAMMABILE CON UN CLICK

Il sistema nasce per cercare contenuti contro i minori. Ma l'infrastruttura tecnica che viene costruita — un filtro automatico installato sul dispositivo di ogni utente, capace di analizzare qualsiasi contenuto prima dell'invio — è identica a quella necessaria per intercettare qualsiasi altro tipo di messaggio.

Per estendere la sorveglianza a opinioni politiche, contenuti religiosi, satira, giornalismo investigativo, basta modificare i parametri dell'algoritmo con un paio di click. Non serve un nuovo Regolamento, non serve un nuovo voto: **basta un aggiornamento del software.**

Non è un'ipotesi teorica. La storia della sorveglianza di massa, in Europa e fuori, dimostra che nessun governo ha mai costruito un sistema di intercettazione generalizzata e poi rinunciato ad ampliarne l'uso. Lo strumento crea la tentazione, e la tentazione diventa prassi.

02

SORVEGLIANZA SENZA SOSPETTO

Il principio su cui si fonda il Chat Control è la **scansione preventiva e generalizzata di tutti i messaggi di tutti gli utenti**, indipendentemente da qualsiasi indizio di reato. Non si indaga una persona sospettata: si controllano tutti, nella speranza di trovare qualcuno.

È il rovesciamento del principio su cui si fonda il diritto penale europeo, secondo il quale si indaga dopo un sospetto, non prima. Lo stesso principio in base al quale la Corte di Giustizia dell'UE ha già bocciato i sistemi di conservazione generalizzata dei dati.

Il Garante europeo per la protezione dei dati (EDPS) e il Comitato europeo (EDPB) hanno definito la proposta "**sproporzionata**", avvertendo che essa "potrebbe diventare la base per una scansione generalizzata e indiscriminata del contenuto di praticamente tutti i tipi di comunicazione elettronica".⁽¹⁾

03

FALSI POSITIVI: INNOCENTI SEGNALATI COME POSSIBILI CRIMINALI

Gli algoritmi producono errori. Applicati a miliardi di messaggi al giorno, anche un tasso di errore piccolo genera un numero enorme di segnalazioni errate. Con implicazioni potenzialmente devastanti.

LE CIFRE — PAESE PER PAESE

I dati provengono dalle segnalazioni automatiche inviate dal National Center for Missing and Exploited Children (NCMEC) americano alle polizie europee e dalle dichiarazioni delle stesse autorità.

Germania — La Polizia criminale federale (Bundeskriminalamt, BKA) ha reso noto che nel 2024 **il 48%** delle 205.728 segnalazioni ricevute dal NCMEC — cioè 99.375 — **non aveva rilevanza penale**. Un dato in crescita rispetto al 2023, quando i falsi positivi erano già 90.950.⁽²⁾

Svizzera — La Polizia federale (Fedpol) ha dichiarato che circa **l'80%** delle segnalazioni automatiche ricevute era privo di rilevanza penale. Tra i contenuti segnalati per errore: foto di vacanza con bambini al mare.⁽³⁾

Irlanda — Dei 4.192 rapporti ricevuti dalla polizia irlandese (An Garda Síochána), solo 852 — **il 20%** — riguardavano effettivamente materiale di abuso. 471 segnalazioni (l'11%) erano falsi positivi accertati.⁽⁴⁾

Unione Europea — La stessa ex Commissaria europea agli Affari interni, Ylva Johansson, ha ammesso che **il 75%** delle chat segnalate nella UE — circa 300.000 all'anno — **non è utilizzabile dalle forze dell'ordine**.⁽⁵⁾

Questi numeri significano una cosa sola: gli algoritmi segnalano centinaia di migliaia di cittadini innocenti, sommergendo gli investigatori sotto una valanga di falsi allarmi e distogliendoli dalle indagini reali sui criminali.

Foto di famiglia, immagini mediche, conversazioni tra genitori possono essere automaticamente segnalate e inoltrate alle forze dell'ordine. Il risultato non è più sicurezza: è meno sicurezza, perché le risorse investigative vengono distolte dalle indagini reali.

CHI SI È ESPRESSO CONTRO IL CHAT CONTROL

Il Garante europeo della protezione dei dati (EDPS) e il Comitato europeo per la protezione dei dati (EDPB) hanno pubblicato un Parere congiunto nel luglio 2022 in cui definiscono la proposta **"sproporzionata"** e avvertono che essa rischia di instaurare una **"sorveglianza di massa"** delle comunicazioni private nell'intera Unione Europea.⁽¹⁾

Il Servizio giuridico del Consiglio dell'Unione Europea — l'organo che consiglia i governi sulla legalità delle norme — ha redatto un parere riservato (trapelato nel 2023) in cui conclude che la proposta è **probabilmente incompatibile con i diritti fondamentali** sanciti dalla Carta dell'UE, in particolare con il diritto alla vita privata e alla protezione dei dati personali.⁽⁶⁾

Oltre 800 scienziati e ricercatori di 37 Paesi — esperti di crittografia, sicurezza informatica e intelligenza artificiale — hanno firmato una lettera aperta in cui definiscono il client-side scanning **"tecnicamente irrealizzabile senza compromettere la sicurezza"** e un **"pericolo per la democrazia"**.⁽⁷⁾

Signal, Mozilla, Proton Mail e Tuta (ex Tutanota) — tra le principali aziende tecnologiche impegnate nella difesa della privacy — hanno dichiarato pubblicamente che il Chat Control **mina alla base la crittografia end-to-end** e crea vulnerabilità di sicurezza sfruttabili da hacker e governi autoritari. La presidente di Signal, Meredith Whittaker, ha annunciato che l'app cesserebbe di operare nell'UE piuttosto che introdurre una backdoor.

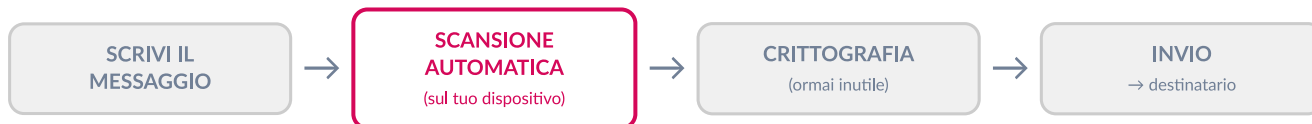
Germania, Paesi Bassi, Polonia, Austria e Lussemburgo — tra gli altri — hanno espresso contrarietà o forti riserve in sede di Consiglio dell'UE, contribuendo in più occasioni a impedire il raggiungimento della maggioranza qualificata necessaria per approvare il mandato negoziale.

La scansione è dentro il tuo telefono

Esiste un motivo per cui milioni di persone usano WhatsApp o Signal per le comunicazioni più riservate: la crittografia end-to-end. Significa che il messaggio viene cifrato sul dispositivo di chi lo invia e decifrato solo sul dispositivo di chi lo riceve. Nemmeno l'azienda che gestisce il servizio può leggerlo.

Il Chat Control 2.0 aggira questa garanzia di privacy con una tecnica chiamata "client-side scanning" — letteralmente, la scansione lato cliente. In pratica: l'algoritmo di controllo viene installato direttamente sul tuo dispositivo e analizza il contenuto del messaggio prima che venga crittografato e inviato.

Non è una metafora, è il funzionamento tecnico previsto dal Regolamento. La crittografia resta formalmente intatta — nessuno la "rompe" — ma diventa inutile, perché il contenuto viene letto prima di essere protetto.



È come mettere una lettera in cassaforte dopo che qualcuno ne ha già fotografato il contenuto.

PERCHÉ GLI ESPERTI LO CHIAMANO BACKDOOR

Una **backdoor** è un accesso nascosto che aggira le protezioni di sicurezza di un sistema. Gli esperti di sicurezza informatica — compreso il comitato scientifico indipendente della Commissione Europea — avvertono che il client-side scanning è **tecnicamente indistinguibile da una backdoor**.⁽⁸⁾

Un sistema di scansione installato su centinaia di milioni di dispositivi diventa un bersaglio per hacker, servizi di intelligence stranieri e governi autoritari. Se il filtro può essere aggiornato da remoto per cercare contenuti pedopornografici, può essere aggiornato da remoto per cercare qualsiasi altra cosa.

Apple aveva annunciato nel 2021 un sistema simile per iPhone. Lo ha ritirato pochi mesi dopo, dichiarando che non era possibile garantirne la sicurezza e che il rischio di abusi era troppo elevato.

Non è possibile costruire una porta che si apra solo per i "buoni". Se la porta esiste, prima o poi qualcun altro la troverà.

(8) Cfr. Apple, sospensione del sistema CSAM Detection, dic. 2022; Internet Society, posizione ufficiale sul client-side scanning; Electronic Frontier Foundation (EFF), analisi tecnica.

Come funziona la decisione

Il Chat Control segue il procedimento legislativo ordinario dell'Unione Europea, che coinvolge tre istituzioni.

La Commissione Europea ha presentato la proposta di Regolamento CSAR nel maggio 2022. Il Parlamento Europeo, eletto dai cittadini, e il Consiglio dell'Unione Europea, dove siedono i rappresentanti dei governi dei 27 Stati membri, negoziano ciascuno la propria posizione e poi si confrontano tra loro nei cosiddetti

"triloghi": negoziati a tre tra Parlamento, Consiglio e Commissione, il cui scopo è raggiungere un accordo sul testo finale. Se il trilogio produce un compromesso, il testo concordato viene sottoposto al voto di conferma di Consiglio e Parlamento (che ha la parola finale).

Il tavolo dove si gioca la partita politica più importante è il **Consiglio dell'Unione Europea**. È lì che i governi nazionali esprimono il loro voto. Su questo dossier si riuniscono, in particolare, i delegati dei 27 governi responsabili nei settori della Giustizia e degli Interni. Per l'Italia, dunque, siedono a quel tavolo il Ministro della Giustizia e il Ministro dell'Interno, attualmente Carlo Nordio e Matteo Piantedosi. La posizione con cui l'Italia si presenta al Consiglio è però coordinata dal **Ministro per gli Affari Europei**, attualmente Tommaso Foti, che ne è il responsabile politico.

COME SI VOTA E COME SI BLOCCA

Per **approvare** il Chat Control al Consiglio serve una **maggioranza qualificata**: almeno 15 Stati membri che rappresentino il 65% della popolazione dell'UE.

Per **bloccarlo** basta una **"minoranza di blocco"**: 4 Stati che rappresentino oltre il 35% della popolazione.

L'Italia da sola non raggiunge la soglia di blocco (rappresenta circa il 13% della popolazione UE). Ma è il terzo Paese per abitanti e il suo voto contrario è politicamente decisivo: rende molto più facile costruire una minoranza di blocco con altri tre o quattro Stati.

Per questo la posizione del Governo italiano pesa più di quanto il numero suggerisca. E per questo chiediamo che sia una posizione di netta contrarietà.

Note: (1) EDPB-EDPS, Joint Opinion 04/2022 sulla proposta CSAR, luglio 2022. (2) Bundeskriminalamt (BKA), Rapporto annuale 2024 sulle segnalazioni NCMEC CyberTipline. (3) Polizia federale svizzera (Fedpol), dati citati nella lettera aperta dei ricercatori, 2024. (4) Dati An Garda Síochána (polizia irlandese), 2020. (5) Dichiarazioni dell'ex Commissaria europea agli Affari interni Ylva Johansson. (6) Parere del Servizio giuridico del Consiglio dell'UE, trapelato 2023. (7) Lettera aperta, oltre 800 scienziati di 37 Paesi — csa-scientist-open-letter.org. (8) Cfr. Apple, sospensione del sistema CSAM Detection, dicembre 2022; Internet Society, posizione ufficiale sul client-side scanning; Electronic Frontier Foundation (EFF), analisi tecnica.

Cosa puoi fare **tu**

Questo documento è nelle tue mani perché qualcuno ha deciso che la tua privacy vale più del silenzio. **Ora tocca a te.**

Nessuna legge ingiusta è mai stata fermata dal consenso passivo dei cittadini. Il Chat Control avanza perché la maggior parte delle persone non sa che esiste, non sa che il proprio Governo ha già votato a favore, e non sa che un negoziato decisivo è in corso proprio adesso a Bruxelles. **L'arma più potente contro una legge che nasce nell'ombra è la luce dell'informazione.**

Il primo passo è quello che hai appena fatto: **informarti**. Il secondo è altrettanto semplice e altrettanto decisivo: **far arrivare questo documento a più persone possibile** — familiari, amici, colleghi, gruppi WhatsApp, social network. Ogni persona che scopre cos'è il Chat Control è una persona in meno che accetterà in silenzio di essere sorvegliata. Il terzo passo è aggiungere il tuo nome a quelli di migliaia di italiani che hanno già detto basta: **firma la petizione** e chiedi al Governo italiano di opporsi. Le firme non restano in un server: vengono consegnate fisicamente al Ministero per gli Affari Europei.

La tua privacy è sotto attacco. Ma non è ancora persa. Dipende da quello che fai adesso.

1

INFORMATI

Hai appena letto questo documento. Ora sai cos'è il Chat Control, cosa prevede e perché ti riguarda. È già il passo più importante.

2

DIFFONDI

Inoltra questo documento a tutti i tuoi contatti. Condividilo nei gruppi WhatsApp, su Telegram, sui social. Il Chat Control avanza nel silenzio: rompi il silenzio.

3

FIRMA LA PETIZIONE

Aggiungi la tua firma a quelle di migliaia di italiani. Le firme vengono consegnate di persona al Ministro per gli Affari Europei. La tua voce conta.

FIRMA ORA LA PETIZIONE

provitaefamiglia.it/petizione/fermiamo-il-chat-control



Inquadra il QR con la fotocamera del telefono



www.provitaefamiglia.it

info@provitaefamiglia.it