FAQ su Chat Control

12 luglio 2026

https://www.peacelink.it/cybercultura/

📌 FAQ: Chat Control e riservatezza delle chat in Europa

1. Che cos'è il "Chat Control"?

È il soprannome dato dai critici e dai media a un filone di normative dell'Unione Europea nate con l'obiettivo di contrastare la diffusione del materiale pedopornografico online (CSAM). Il nome ufficiale usato nei documenti dell'UE è *Child Sexual Abuse Regulation* (CSAR).

2. Qual è la differenza tra Chat Control 1.0 e Chat Control 2.0?

- **Chat Control 1.0 (Regolamento UE 2021/1232):** è la norma attualmente in vigore, prorogata fino al 3 aprile 2028. Consente ai fornitori di servizi di scansionare i messaggi dei propri utenti su base puramente volontaria.
- **Chat Control 2.0 (Proposta di Regolamento CSAM):** è il progetto di legge permanente ancora in discussione. Se approvato, introdurrà ordini di rilevamento obbligatori, costringendo legalmente le piattaforme a effettuare le scansioni.

3. A quale legge deroga il Chat Control attuale?

Deroga alla Direttiva ePrivacy (2002/58/CE). In particolare, sospende temporaneamente l'applicazione degli articoli che garantiscono la riservatezza delle comunicazioni e l'obbligo di cancellazione immediata dei dati sul traffico. Senza questa deroga, le scansioni automatiche compiute dalle piattaforme sarebbero illegali.

4. Quali Paesi europei si oppongono alla versione obbligatoria (Chat Control 2.0)?

La proposta ha spaccato il Consiglio dell'Unione Europea. La Germania guida il fronte del "No", ritenendo lo screening una violazione della propria Costituzione. Nazioni come l'Austria, la Polonia, i Paesi Bassi e l'Estonia si oppongono fermamente per proteggere la crittografia. L'Italia mantiene una posizione più cauta, sollevando perplessità tecniche sulla sicurezza delle infrastrutture, mentre la Francia e la Spagna si sono mostrate più favorevoli.

5. Come funzionano i database degli hash per la scansione?

Il sistema si basa sul confronto matematico dei file senza che un operatore umano debba leggere i messaggi privati:

- **Generazione:** ogni file digitale ha un'impronta digitale univoca chiamata "hash".
- **Archivio:** organizzazioni come il NCMEC o Europol gestiscono database protetti contenenti solo gli hash di materiale pedopornografico già noto.
- **Confronto:** quando un utente invia una foto, la piattaforma calcola il suo hash e lo confronta in automatico con il database. Se non c'è corrispondenza, il messaggio prosegue; se c'è un riscontro positivo, il file viene bloccato e verificato dal team di sicurezza prima della segnalazione alle forze dell'ordine.

6. Che cos'è il *Client-Side Scanning* e perché fa discutere?

Molte app usano la crittografia end-to-end, che impedisce ai server delle aziende di leggere i messaggi. Per aggirare questo ostacolo, il Chat Control 2.0 vorrebbe imporre l'installazione di un software direttamente sullo smartphone dell'utente, capace di scansionare foto, video e testi prima che vengano crittografati e inviati. Gli esperti di sicurezza informatica lo considerano una grave minaccia alla cybersicurezza globale.

7. Perché questa tecnologia non viene applicata anche per combattere le mafie?

L'Unione Europea esclude questa estensione per tre motivi principali:

- **Diritto e proporzionalità:** la tutela dei minori è considerata un'eccezione estrema. Allargare lo strumento a reati associativi creerebbe una sorveglianza di massa indiscriminata, vietata dalla Corte di Giustizia UE.
- **Natura del contenuto:** la lotta alla pedopornografia cerca immagini note (hash). La mafia si muove tramite messaggi di testo e linguaggio cifrato; per intercettarla servirebbe un'Intelligenza Artificiale invasiva capace di interpretare il testo di ogni cittadino, con enormi rischi di falsi positivi.
- **Strumenti già esistenti:** per combattere le mafie, la magistratura usa già intercettazioni mirate e Trojan di Stato, che colpiscono singoli sospettati tramite mandato del giudice, anziché monitorare preventivamente l'intera popolazione.

📖 Glossario dei termini chiave

- **Chat Control:** termine giornalistico e politico utilizzato per indicare le iniziative legislative dell'Unione Europea volte a monitorare le comunicazioni digitali private per contrastare gli abusi sui minori.
- **Client-Side Scanning (Scansione lato client):** tecnologia che prevede l'analisi automatica dei file (immagini, testi, video) direttamente sul dispositivo dell'utente (smartphone, PC) prima che vengano inviati o protetti da crittografia.
- **Crittografia End-to-End (E2EE):** sistema di comunicazione cifrata in cui solo gli utenti che comunicano possono leggere i messaggi. Impedisce a terzi, inclusi i fornitori di servizi internet e i gestori delle piattaforme, l'accesso alle chiavi di lettura del testo o dei file.
- **CSAM (Child Sexual Abuse Material):** acronimo internazionale utilizzato nei documenti legali e tecnici per definire il materiale pedopornografico o relativo all'abuso sessuale sui

minori.
- **CSAR (Child Sexual Abuse Regulation):** nome ufficiale della proposta di regolamento europeo avanzata dalla Commissione Europea per prevenire e combattere l'abuso sessuale online sui minori.
- **Direttiva ePrivacy:** normativa dell'Unione Europea (Direttiva 2002/58/CE) che tutela il diritto alla vita privata, alla riservatezza delle comunicazioni e alla protezione dei dati personali nel settore delle comunicazioni elettroniche.
- **Europol:** agenzia dell'Unione Europea per la cooperazione nell'attività di contrasto della criminalità, che supporta gli Stati membri nella lotta ai crimini internazionali e al terrorismo.
- **Falso positivo:** errore di un sistema informatico di monitoraggio che scambia erroneamente un file o un testo lecito per un contenuto illegale, attivando una falsa segnalazione di allarme.
- **Hash:** stringa univoca di lettere e numeri generata da un algoritmo matematico che funge da "impronta digitale" per identificare in modo univoco un file informatico, senza rivelarne direttamente il contenuto visivo o testuale.
- **NCMEC (National Center for Missing & Exploited Children):** organizzazione non profit statunitense che coordina le segnalazioni globali di materiale pedopornografico online e collabora con le forze dell'ordine di tutto il mondo.
- **Trojan di Stato (Malware di Stato):** software spia (intercettatore informatico) utilizzato legalmente dalle forze dell'ordine, dietro autorizzazione della magistratura, per infettare un dispositivo bersaglio e monitorarne le attività in tempo reale.

Le posizioni ufficiali delle grandi aziende tech

Le aziende tecnologiche si dividono in **due fronti opposti**, a seconda del modello di business e, soprattutto, dell'architettura di sicurezza che utilizzano per proteggere i dati.

Si assiste a un vero e proprio scontro tra i colossi del web tradizionali e i gestori delle applicazioni focalizzate sulla privacy.

FRONTE A: le app ultra-sicure (Signal, WhatsApp, Proton Mail)

Queste aziende si oppongono fermamente a qualsiasi forma di obbligo (Chat Control 2.0) e minacciano misure estreme.

- **Signal:** la presidente della Signal Foundation, Meredith Whittaker, ha dichiarato ripetutamente che Signal **lascerà completamente il mercato europeo** piuttosto che inserire una backdoor o attivare il *client-side scanning*. La posizione dell'azienda è netta:

un sistema crittografato o è sicuro per tutti o non lo è per nessuno. [1, 2, 3, 4]
- **WhatsApp:** il capo di WhatsApp presso Meta, Will Cathcart, ha espresso una posizione identica a quella di Signal. WhatsApp si rifiuterà di conformarsi a leggi che impongono di rompere o aggirare la crittografia end-to-end per i cittadini europei, preferendo rischiare il blocco dell'applicazione. [1, 2, 5]
- **Proton (Proton Mail, Proton VPN):** l'azienda svizzera combatte attivamente la proposta, definendola una minaccia alla democrazia e alla sicurezza informatica. Secondo Proton, creare una vulnerabilità di Stato significa consegnare una chiave di accesso anche a hacker e governi autoritari. [4, 5]

La loro argomentazione tecnica principale è che **non esiste una via di mezzo**: non si può creare un sistema di scansione che legga i messaggi prima che vengano crittografati senza distruggere l'essenza stessa della sicurezza e del segreto industriale. [1, 6]

FRONTE B: i colossi del web tradizionali (Google, Meta per Messenger/Instagram, Microsoft, Snap)

Queste aziende hanno una posizione molto diversa: supportano fortemente la possibilità di effettuare scansioni e, anzi, hanno protestato duramente quando la legge ha subito dei rallentamenti. [7, 8]

- **La protesta contro il vuoto normativo:** quando la deroga temporanea di Chat Control 1.0 è brevemente decaduta prima del rinnovo fino al 2028, colossi come Google, Meta, Snap e Microsoft hanno apertamente criticato l'Unione Europea. Hanno definito il mancato accordo tempestivo un "fallimento irresponsabile". [8, 9]
- **Il motivo del supporto:** queste piattaforme gestiscono servizi che in gran parte non usano la crittografia end-to-end di default (come le email di Gmail o le chat di Instagram e Facebook Messenger). Utilizzano già da anni software automatizzati sui propri server per individuare abusi e pedopornografia. [1, 10]
- **La richiesta di copertura legale:** il loro obiettivo principale è ottenere una **tutela giuridica certa** (quella offerta dalla deroga attuale). Senza di essa, rischiano di essere denunciate dagli utenti europei per violazione della privacy ogni volta che i loro algoritmi scansionano una foto o un testo. [1, 9, 10, 11]

In sintesi

Il panorama industriale è spaccato a metà: da un lato ci sono le aziende che basano il proprio business sulla **raccolta controllata e sulla moderazione dei contenuti** (che chiedono tutele legali per continuare a scansionare sui server); dall'altro ci sono le aziende che basano tutto sulla **riservatezza matematica** (che vedono nel Chat Control obbligatorio un pericolo mortale per la sicurezza globale dei dati). [2, 6, 9, 10, 12]

Fonti

[1] https://www.youtube.com
[2] https://www.youtube.com
[3] https://www.wired.it
[4] https://www.forbes.com
[5] https://nextcloud.com
[6] https://www.youtube.com
[7] https://www.cio.com
[8] https://www.theguardian.com
[9] https://therecord.media
[10] https://www.linkedin.com
[11] https://www.newsweek.com
[12] https://mailchimp.com