383

20 ottobre 2025

IBL Focus

Chat control: il conflitto tra sicurezza dei minori e tutela della privacy nell'Unione Europea

Di Claudia Giulia Ferrauto

1. Introduzione

La proposta dell'Unione Europea nota come chat control, introdotta nel 2020 e formalizzata nel 2022, mira a contrastare la diffusione di materiale di abuso sessuale su minori (CSAM[1]) e l'adescamento online di minori (*grooming*)[2] , imponendo ai fornitori di servizi digitali (piattaforme di messaggistica, email e cloud) la scansione automatica dei contenuti, anche quelli protetti da crittografia end-to-end (E2EE[3]).

Sebbene la tutela dei minori sia un obiettivo prioritario, la proposta solleva gravi preoccupazioni per la sua natura di sorveglianza di massa incompatibile con i diritti fondamentali sanciti dagli articoli 7 (riservatezza delle comunicazioni) e 8 (protezione dei dati personali) della Carta dei diritti fondamentali dell'UE.

La giurisprudenza della Corte di giustizia dell'Unione Europea considera tali misure sproporzionate[4].

Claudia Giulia Ferrauto è analista indipendente in comunicazione e tecnologia, ha collaborato con Il Foglio e Il Sole 24 Ore. Autrice di "Intelligenza Artificiale: cos'è davvero" (Bollati Boringhieri).

1. **CSAM**: è l'acronimo di Child Sexual Abuse Material, ovvero immagini, video o altri contenuti digitali che mostrano abusi sessuali su minori. Questi materiali sono illegali e rappresentano una grave violazione dei diritti dei bambini.
2. **Grooming online**: si chiama così l'adescamento di minori tramite piattaforme digitali, come chat o social media, in cui un adulto - fingendosi spesso un'altra persona e/o un utente di pari età di chi intende adescare- cerca di instaurare un rapporto di fiducia con un minore per scopi illeciti, spesso di natura sessuale.
3. **E2EE**: è l'acronimo di End-to-End Encryption, ed è un tipo di crittografia in cui solo il mittente e il destinatario possono leggere i messaggi scambiati. Nemmeno il servizio che gestisce la comunicazione (es: WhatsApp o Signal) può accedere al contenuto, perché i dati sono criptati già sul dispositivo del mittente e vengono decriptati solo su quello del destinatario.
4. Si vedano per esempio le sentenze Schrems II e Quadrature du Net. **Schrems II** (C-311/18): è una sentenza della Corte di giustizia dell'UE che ha invalidato un accordo per il trasferimento di dati tra UE e USA perché non garantiva protezione adeguata contro la sorveglianza. **Quadrature du Net** (C-623/17): è una sentenza della Corte di giustizia dell'UE che ha stabilito che la raccolta indiscriminata di dati personali (es. le comunicazioni) è illegale, salvo casi eccezionali

Le tecnologie previste per l'analisi dei contenuti, come il client-side scanning[5], presentano rischi di falsi positivi, vulnerabilità di sicurezza ed espansione delle finalità di sorveglianza[6] (function creep).

Inoltre, la proposta potrebbe spingere aziende tecnologiche a lasciare il mercato europeo, con danni per l'innovazione, nonché legittimare le analoghe azioni di regimi autoritari che ovviamente usano queste tecniche per ragioni assai meno nobili della tutela dei minori , normalizzando la sorveglianza globale.

Nel giorno del voto che tutti tenevano sottocchio di recente, previsto in origine per il 14 ottobre 2025, ma posticipato a data da definirsi per mancanza di consenso, si raccomanda di rigettare la proposta attuale, eventualmente valutando soluzioni alternative come la crittografia omomorfica (che consente di eseguire operazioni su dati cifrati senza doverli decifrare)[7] e la cooperazione transnazionale

giustificati.

5. **Client-side scanning**: si tratta di una tecnologia che analizza i contenuti (es. foto, video, messaggi) direttamente sul dispositivo dell'utente (es. smartphone) prima che questi vengano cifrati, per essere poi inviati tramite canali che prevedono la crifratura (es: whatsapp) permettendo al sistema di rilevare materiale ritenuto - dal software di analisi - illecito, compromettendo la privacy di tutti gli utenti indipendentemente dall'esito della procedura.
6. **Function creep**: si parla di FC quando si intende estendere l'uso di dati raccolti per uno scopo (es. trovare CSAM) per scopi diversi da quello originario, quindi per scopi non previsti, come il monitoraggio di attività politiche o di altro tipo.
7. **Crittografia omomorfica**: è una tecnica avanzata che permette di eseguire operazioni su dati cifrati senza doverli decifrare. Questo significa che è possibile fare calcoli, ricerche o analisi su informazioni (file, messaggi, immagini) che restano sempre protette e illeggibili per chi le elabora, garantendo così un elevato livello di privacy e sicurezza. Un esempio semplice che può aiutare a chiarire il concetto. Immaginate che tre persone – A, B e C – vogliano sapere qual è la somma dei loro risparmi, ma senza rivelare a nessuno quanto possiede ognuno di loro. Ciascuno condivide il proprio importo usando la crittografia omomorfica, e poi lo invia a un server. Il server, pur non avendo accesso ai dati (in questo caso, numeri) originali, può comunque eseguire la somma dei diversi valori cifrati. Alla fine, qualcuno con la chiave di decifratura potrà leggere il totale – nel nostro esempio, 450 euro – ma senza che in nessun momento siano stati visibili i singoli importi. Questa tecnologia è particolarmente utile in situazioni in cui la riservatezza è fondamentale, come ad esempio nell'analisi di dati sanitari, nelle indagini giudiziarie, in servizi finanziari o nei servizi cloud che devono eseguire operazioni su dati sensibili senza poterli mai leggere. Quindi è possibile cercare contenuti illeciti all'interno di messaggi cifrati, senza mai decifrarli, quindi senza violare la privacy degli utenti. Un altro esempio per capire intuitivamente il funzionamento della crittografia omomorfica è immaginare di cucinare una torta indossando degli occhiali opachi. Non puoi vedere gli ingredienti, ma riesci comunque a mescolarli e a cuocerli. Solo alla fine, una volta che si ha modo di togliere gli occhiali, si vede la torta finita. Allo stesso modo, la crittografia omomorfica permette di "lavorare" su dati invisibili, ottenendo alla fine un risultato corretto, ma visibile solo a chi ha l'autorizzazione per decifrarlo. Rispetto alla crittografia tradizionale, che protegge i dati solo durante il trasporto o l'archiviazione - ma che richiede di decifrarli per poterli usare - la crittografia omomorfica rappresenta un passo avanti poiché consente di mantenere i dati cifrati in ogni fase, anche durante l'elaborazione, riducendo drasticamente i rischi di esposizione.

per bilanciare sicurezza e diritti fondamentali[8].

2. Contesto e sviluppo normativo europeo

La proposta di regolamento per prevenire e combattere l'abuso sessuale su minori (CSAR[9]), nota come chat control, è stata presentata dalla Commissione Europea nel maggio 2022[10] come evoluzione di una deroga temporanea alla direttiva ePrivacy[11]. Quest'ultima consentiva ai provider di servizi digitali di scansionare volontariamente contenuti non cifrati per rilevare CSAM.

La nuova proposta introduce obblighi di scansione automatica, anche per comunicazioni protette da E2EE, coinvolgendo piattaforme di messaggistica come WhatsApp, Signal e Telegram, oltre a servizi di email e cloud.

L'iniziativa risponde all'aumento degli abusi online: nel 2021, oltre 85 milioni di immagini e video di CSAM sono stati segnalati globalmente, molti su reti cifrate[12].

La Commissione ha proposto l'istituzione di un EU Centre to Prevent and Combat Child Sexual Abuse per coordinare segnalazioni e indagini, centralizzando i dati raccolti dai provider.

Il dibattito politico, iniziato nel 2020, si è dunque intensificato con Chat Control 2.0 nel 2022, proposto dalla Commissaria per gli Affari interni Ylva Johansson.

Due rifiuti nel 2024 (giugno e dicembre) per mancanza di maggioranza qualificata nel Consiglio UE ne hanno ritardato l'adozione[13].

La presidenza danese dell'UE, iniziata il 1° luglio 2025, ha rilanciato una versione più stringente, con un voto cruciale previsto in origine per il 14 ottobre 2025.

Tuttavia, le critiche da parte di giuristi, aziende tecnologiche, garanti nazionali della privacy e organizzazioni per i diritti digitali, come European Digital Rights (EDRi) e Electronic Frontier Foundation (EFF)[14], sottolineano i rischi per la riservatezza

8. https://www.eff.org/deeplinks/2025/09/chat-control-back-menu-eu-it-still-must-be-stopped-0
9. CSAR: è l'acronimo di Child Sexual Abuse Regulation. La CSAR è una proposta legislativa dell'Unione Europea, avanzata dalla Commissione Europea nota come chat control, la quale ha gli obiettivi di 1) prevenire l'abuso sessuale online e offline su minori; 2) obbligare le piattaforme digitali (come app di messaggistica, social network, provider di hosting e servizi di comunicazione) a rilevare, segnalare e rimuovere contenuti di abuso sessuale su minori; 3) un Centro Europeo per contrastare questi crimini.
10. COM/2022/209.
11. Regolamento 2020/2656 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0209
12. https://edri.org/our-work/chat-control-what-is-actually-going-on/
13. https://www.patrick-breyer.de/en/posts/chat-control/
14. EDRi: acronimo di European Digital Rights, è un'associazione che riunisce organizzazioni europee per promuovere e difendere i diritti digitali, come la privacy e la libertà di espressione online. EFF: è l'acronimo di Electronic Frontier Foundation, un'organizzazione internazionale che si occupa di proteggere le libertà digitali, opponendosi a leggi che minacciano la privacy o la sicurezza online.

delle comunicazioni, la sicurezza digitale e la libertà di espressione[15].

3. Obiettivi dichiarati e ratio giuridica

Il regolamento chat control mira a rafforzare la lotta contro CSAM e il grooming online attraverso un quadro normativo vincolante per i fornitori di servizi digitali.

I principali obiettivi delineati[16] includono:

- rilevare e segnalare contenuti illeciti tramite tecnologie automatizzate, anche su comunicazioni cifrate;
- identificare vittime e perseguire penalmente i responsabili;
- obbligare i provider a implementare strumenti di scansione e collaborare con le autorità;
- istituire un EU Centre per gestire segnalazioni e monitorare le misure. Il meccanismo si articola in tre fasi: valutazione del rischio da parte dei provider, **ordini di rilevamento emessi da autorità nazionali per rischi significativi e segnalazione dei contenuti rilevati con successiva rimozione e notifica alle forze dell'ordine.**

L'approccio generalizzato e l'assenza di limiti temporali chiari sollevano dubbi sulla proporzionalità e sulla compatibilità con il diritto europeo, come evidenziato da Signal[17].

4. Criticità giuridiche e conflitti con i principi dell'Unione Europea

La proposta di chat control presenta numerose criticità giuridiche che la rendono molto probabilmente incompatibile con i principi fondamentali dell'Unione Europea, minacciando privacy, sicurezza digitale e libertà di espressione. La scansione obbligatoria di tutte le comunicazioni private, incluse quelle protette da crittografia end-to-end, sembra violare l'articolo 7 della Carta dei diritti fondamentali, che garantisce la riservatezza delle comunicazioni. La Corte di giustizia dell'Unione Europea, nelle già citate sentenze Schrems II (C-311/18) e Quadrature du Net (C-623/17), ha stabilito che la sorveglianza di massa è sproporzionata e contraria ai principi di necessità e proporzionalità, trattando ogni utente come sospetto[18].

Il client-side scanning, che accede ai contenuti prima della crittografia, compromette l'E2EE, pilastro della sicurezza digitale secondo l'Agenzia dell'UE per la cybersicurezza (ENISA), introducendo vulnerabilità, come dimostrato dall'attacco hacker noto come Salt Typhoon[19].

Una lettera aperta di centinaia di scienziati nel settembre 2025 ha definito la pro-

15. https://tuta.com/blog/chat-control-criticism
16. COM/2022/209.
17. https://signal.org/blog/pdfs/germany-chat-control.pdf
18. vedi nota 4.
19. Salt Typhoon: si tratta di un attacco informatico che ha sfruttato vulnerabilità note nei firewall, nei router, nei prodotti VPN, quindi nei sistemi di comunicazione, dimostrando in questo i rischi dietro accessi nascosti https://www.tenable.com/blog/salt-typhoon-an-analysis-of-vulnerabilities-exploited-by-this-state-sponsored-actor .

posta tecnicamente infattibile senza minare la sicurezza digitale.[20]

Inoltre, la raccolta massiva di dati personali e il loro trasferimento al EU Centre violano i principi di minimizzazione e consenso informato del GDPR (articolo 5), aumentando i rischi di abuso, come sottolineato dal Garante italiano per la protezione dei dati.[21]

L'indeterminatezza normativa apre al rischio di eccedere rispetto alle finalità di sorveglianza[22], con possibili estensioni della sorveglianza a temi come la "disinformazione". L'emissione di ordini di rilevamento senza controllo giurisdizionale contrasta con la giurisprudenza della Corte europea dei diritti dell'uomo[23] e della Corte di giustizia dell'UE.

Infine, la sorveglianza generalizzata può generare conseguenze anche sul comportamento delle persone, spaventate dalla percezione di essere sempre sorvegliati, limitando la libertà di espressione di giornalisti, attivisti e whistleblower (chilling effect[24]). In conclusione, la proposta non sembra soddisfare i requisiti di necessità e proporzionalità, rappresentando una minaccia per lo stato di diritto digitale.

5. Rischi tecnologici della proposta di chat control

La proposta contempla l'impiego di strumenti basati sull'intelligenza artificiale, incluse tecnologie di riconoscimento visivo e modelli linguistici computazionali, con l'obiettivo di rilevare e classificare contenuti potenzialmente illeciti. Tecnologie come client-side scanning, machine learning e hashing[25] presentano limiti signifi-

20. https://www.heise.de/en/news/400-scientists-speak-out-against-chat-control-10637109.html
21. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10171128
22. vedi nota 6.
23. Per esempio il caso Zakharov c. Russia, la sentenza del caso della Corte europea dei diritti dell'uomo (CEDU), che ha stabilito che la sorveglianza di massa deve essere soggetta a un controllo giudiziario da parte di un giudice per garantire la conformità con i diritti umani, in particolare il rispetto del diritto alla vita privata, come stabilito dalla Convenzione europea dei diritti dell'uomo. La sentenza ha sottolineato l'importanza dell'autorizzazione giudiziaria per prevenire violazioni di tali diritti fondamentali.
24. Chilling effect: si chiama così l'effetto psicologico per cui le persone, temendo di essere sotto continua osservare, sorvegliate, cambiano il loro comportamento e auto-limitano la loro libertà di espressione, ad esempio evitando di parlare di temi sensibili online o evitando di esprimere opinioni o usare determinati vocaboli. In sostanza è l'effetto "raggelante" che porta individui e gruppi ad astenersi dall'esercitare un proprio diritto, come la libera espressione, per paura di ritorsioni, sanzioni legali o altre conseguenze negative.
25. Hashing; usato come tecnica di analisi dei contenuti è un processo che trasforma un contenuto digitale (es. immagine, video, testo) in una stringa unica di caratteri (hash) tramite un algoritmo (es. MD5, SHA-256). Questa stringa funge da impronta digitale del contenuto, permettendo di identificare rapidamente file identici o simili senza analizzarne direttamente il contenuto. È usato, ad esempio, per rilevare contenuti illegali o duplicati confrontando gli hash con un database di hash noti. Perché è facile da aggirare: questo tipo di analisi è vulnerabile perché anche piccole modifiche al contenuto (es. cambio di un pixel in un'immagine, ruotare una foto o la modifica di una parola in un testo) generano un

cativi. Gli algoritmi di intelligenza artificiale infatti possono generare falsi positivi, classificando erroneamente contenuti leciti come illeciti, con conseguenti violazioni della privacy e messa in osservazione di cittadini innocenti, senza contare l'inutile, se non addirittura dannoso, sovraccarico di segnalazioni per le autorità[26].

I metodi necessari ad aggirare i normali sistemi di autenticazione ed eseguire la scansione, possono essere backdoor tecniche[27], che espongono i sistemi a cyberattacchi, come evidenziato da Signal, compromettendo le infrastrutture critiche[28].

Il rischio di function creep, cioè di eccedere rispetto alle finalità della misura, renderebbe concreto il rischio di un'espansione delle finalità di sorveglianza senza controlli democratici.[29]

Inoltre, l'uso di algoritmi proprietari privi di audit indipendenti può ridurre la trasparenza e aumenta il rischio di bias (cioè di distorsioni o pregiudizi impliciti nel modo in cui vengono effettuate le verifiche sulla liceità dei contenuti). Nello specifico, l'uso di algoritmi proprietari, il cui funzionamento interno, codice e dati di addestramento non sono noti al pubblico né verificabili da terze parti, può rappresentare un problema serio soprattutto in un contesto così delicato dove la trasparenza è fondamentale e si può aumentare il rischio di pregiudizi. In questo senso possiamo definire un sistema di controllo basato su algoritmi - senza audit indipendenti - una sorta di "scatola nera" che impedisce a chiunque, al di fuori dei proprietari e dei loro collaboratori, di capire come vengono prese le decisioni, rendendo difficile verificare se l'algoritmo operi in modo etico e conforme alle normative. Senza audit indipendenti, tecnici, ricercatori o attivisti esperti, non possono controllare o segnalare o correggere eventuali distorsioni derivanti da input o pregiudizi storici incorporati nell'addestramento dell'algoritmo stesso. Ciò può avere gravi conseguenze, specialmente in ambiti delicati come giustizia o servizi sociali, portando a discriminazioni ingiustificate. Gli audit esterni sono quindi fondamentali per identificare e mitigare questi pregiudizi, monitorare costantemente il funzionamento degli algoritmi, garantire la conformità alle normative e rafforzare la fiducia degli utenti. In assenza di trasparenza e controlli indipendenti, il rischio è

hash completamente diverso. Chi vuole eludere il rilevamento può quindi alterare leggermente il file (es. ridimensionando un'immagine o aggiungendo rumore) senza cambiarne il significato, rendendo l'hash non corrispondente a quello originale. Algoritmi di hashing percettivo (es. pHash) cercano di mitigare questo problema, ma non sono infallibili.

26. https://www.eff.org/deeplinks/2025/09/chat-control-back-menu-eu-it-still-must-be-stopped-0

27. Backdoor tecniche: si tratta di vulnerabilità deliberatamente incorporate nel codice di un software, nel firmware o nell'hardware, che consente l'accesso al sistema bypassando i controlli di sicurezza standard (come password, cifratura o autenticazione). A differenza di una vulnerabilità accidentale, la backdoor tecnica è inserita in modo intenzionale, spesso con l'obiettivo di consentire interventi di manutenzione remota, sorveglianza o accesso da parte delle forze dell'ordine, ma una volta in essere può essere trovata e quindi sfruttata anche da soggetti terzi, rendendola un rischio significativo per la sicurezza e la privacy.

28. https://signal.org/blog/pdfs/germany-chat-control.pdf

29. https://www.computerweekly.com/news/366631949/EU-Chat-Control-plans-pose-existential-catastrophic-risk-to-encryption-says-Signal

che decisioni ingiuste e dannose compromettano equità e responsabilità.

Si assisterebbe a un'inversione del principio fondamentale della presunzione d'innocenza: il cittadino non è più considerato non colpevole fino a prova contraria, ma diventa oggetto di un sospetto preventivo, subordinato alla verifica di un sistema algoritmico. Qualora tale sistema commetta un errore, evenienza tutt'altro che infrequente, l'interessato potrebbe essere ingiustamente segnalato, a sua insaputa.

Sembrerebbe quindi che il sistema potrebbe generare più problemi che vantaggi - come sostengono centinaia, tra informatici, giuristi e ricercatori esperti, che hanno scritto alla Commissione presentando le diverse criticità[30].

In sintesi, queste tecnologie minacciano privacy, sicurezza e la stessa affidabilità dei sistemi digitali.

6. Posizioni delle big tech sulla proposta di chat control

La proposta di "Chat Control" ha sollevato forti preoccupazioni anche da parte di numerosi attori dell'industria tecnologica. Aziende come WhatsApp, Apple, Signal, Telegram e X (ex Twitter) hanno espresso un'opposizione netta all'introduzione di sistemi obbligatori di scansione delle comunicazioni cifrate, ritenendo che tali misure metterebbero gravemente a rischio la privacy degli utenti e la sicurezza delle infrastrutture digitali.

Un punto centrale della critica riguarda la minaccia alla crittografia end-to-end, ritenuta fondamentale per proteggere le comunicazioni da accessi non autorizzati. Le Big Tech hanno sostenuto in più occasioni che, al di là dei costi e delle difficoltà tecniche legate al monitoraggio dei messaggi, esistono gravi implicazioni etiche e legali legate alla possibilità che terze parti possano accedere ai contenuti privati degli utenti.

WhatsApp: "Proposta UE pericolosa per la privacy e la sicurezza"

Will Cathcart, CEO di WhatsApp (gruppo Meta), ha definito la proposta della presidenza UE "una minaccia per la privacy e la sicurezza di tutti". Il 3 ottobre 2025 ha dichiarato pubblicamente[31]:

> L'ultima proposta della Presidenza dell'UE viola ancora la crittografia end-to-end, mettendo a rischio la privacy e la sicurezza di tutti, un'opinione condivisa da esperti di oltre 30 paesi. Continuiamo a esortare i paesi dell'UE a impegnarsi per una maggiore sicurezza per i propri cittadini e a respingere questa proposta.

Una posizione ribadita anche nei giorni successivi, segno della forte contrarietà dell'azienda a ogni forma di scansione obbligatoria delle comunicazioni cifrate.

Signal: "Una minaccia esistenziale"

Ancora più drastica è la posizione della Signal Foundation, che ha definito la proposta "una minaccia esistenziale" per la sua missione. Signal ha chiarito che inte-

30. https://www.radio24.ilsole24ore.com/programmi/2024/puntata/novit-chatgpt-e-google--chat-control--pehi--083445-2386855514571452

31. https://x.com/wcathcart/status/1974201213316206758?s=46

grare meccanismi di scansione preventiva nei messaggi - come previsto in alcune versioni del testo normativo- è incompatibile con il proprio modello di sicurezza. L'organizzazione ha dichiarato apertamente che, qualora la normativa venisse approvata nella sua forma attuale, si troverebbe costretta ad abbandonare il mercato europeo.

Non è la prima volta che Signal e WhatsApp ventilano l'ipotesi di ritirarsi da mercati nazionali in risposta a leggi invasive. È il caso, ad esempio, della Svezia, dove entrambe le piattaforme[32] hanno minacciato il ritiro qualora fosse approvata una legge che obbliga alla conservazione dei messaggi privati con accesso per le autorità.

Apple e il precedente del 2021: marcia indietro sullo scanning[33]

Apple ha già vissuto un'esperienza simile nel 2021, quando annunciò l'introduzione di un sistema di scansione lato cliente per individuare materiale pedopornografico (CSAM) nei contenuti destinati a iCloud. L'iniziativa suscitò proteste immediate da parte di gruppi per i diritti civili e di esperti. A seguito del backlash, Apple sospese il progetto a meno di un mese dall'annuncio, riconoscendo le implicazioni per la privacy e la fiducia degli utenti.

Meta e il percorso verso l'E2EE universale

Dal 2019, Meta ha avviato un processo per estendere la crittografia end-to-end a tutte le sue piattaforme di messaggistica[34], incluse Facebook Messenger e Instagram Direct, oltre a WhatsApp dove è già attiva. L'implementazione è stata rallentata da sfide tecniche e problemi di interoperabilità, ma anche da pressioni governative, in particolare dagli Stati Uniti e da altri paesi preoccupati che E2EE possa ostacolare la lotta alla criminalità e alla disinformazione.

Ciononostante, Meta ha mantenuto la rotta. In un rapporto[35] commissionato alla no-profit Business for Social Responsibility (BSR) e pubblicato nel 2022, l'azienda ha evidenziato come la crittografia end-to-end rappresenti una tutela fondamentale dei diritti umani, suggerendo 45 raccomandazioni su come bilanciare sicurezza pubblica e diritto alla privacy.

Telegram: "Un attacco alla libertà"

Il fondatore di Telegram, Pavel Durov, ha diffuso il 14 ottobre 2025 un messaggio[36]. a tutti gli utenti francesi, condannando apertamente la proposta europea. Durov ha denunciato la legge come un tentativo di trasformare i telefoni in strumenti di

32. https://www.ansa.it/canale_tecnologia/notizie/software_app/2025/04/18/whatsapp-e-altre-app-messaggi-minacciano-di-lasciare-la-svezia_d6aba75b-3b2b-406f-9331-1777f807ab13.html?utm_source=chatgpt.com
33. https://www.wired.com/story/apple-icloud-photo-scan-csam-pause-backlash/
34. https://www.redhotcyber.com/post/meta-ha-annunciato-una-transizione-irreversibile-alla-crittografia-e2ee-in-messenger/
35. https://about.fb.com/news/2022/04/expanding-end-to-end-encryption-protects-fundamental-human-rights/
36. https://x.com/durov/status/1978146139175321797?s=46

sorveglianza di massa, accusando direttamente la Francia di guidare l'iniziativa:

> Oggi, l'Unione Europea ha quasi messo al bando il tuo diritto alla privacy [...] Il loro vero obiettivo sono le persone comuni. [...] Solo TU, cittadini comuni, correresti il rischio che i tuoi messaggi e le tue foto private vengano compromessi.

Durov ha attribuito il momentaneo stop della legge all'intervento della Germania, ma ha avvertito che le libertà digitali restano sotto minaccia.

Anche X prende posizione

Infine, X (ex Twitter) ha accolto con favore la decisione del Consiglio dell'UE di rinviare il voto previsto per il 14 ottobre sulla proposta CSAM/Chat Control, definendo[37] il rinvio "un passo importante nella protezione delle comunicazioni sicure". Tuttavia, ha avvertito che la proposta resta sul tavolo, sottolineando l'urgenza di continuare a contrastare qualunque disposizione che legittimi forme di sorveglianza di massa.

In sintesi

Le reazioni di molte delle principali piattaforme digitali, in particolar modo quelle coinvolte direttamente dall'uso di sistemi crittografici, mostrano un fronte comune critico nei confronti della proposta "Chat Control". Pur con sfumature diverse, WhatsApp, Signal, Apple, Telegram, Meta e X hanno espresso timori convergenti: la proposta rappresenta una seria minaccia per la crittografia end-to-end e, più in generale, per i diritti fondamentali alla privacy e alla sicurezza digitale. Di fronte a tali rischi, molte di queste aziende chiedono di valutare soluzioni alternative, in grado di tutelare i minori e contrastare i reati senza compromettere la riservatezza delle comunicazioni.

7. Proposte per bilanciare la protezione dei minori e la tutela dei diritti digitali

Per contrastare il CSAM senza compromettere la privacy e la sicurezza digitale, sarebbe opportuno valutare approcci alternativi alla proposta attualmente in corso di valutazione, che prevedano di limitare le misure a casi specifici e sottoposti a controllo giudiziario, di introdurre clausole di trasparenza e audit indipendenti, nonché di inserire una clausola di revisione periodica.

Per quanto concerne la parte strettamente informatica, andrebbero per esempio usate tecnologie innovative e misure mirate. La scansione indiscriminata (client-side scanning) dovrebbe essere sostituita con indagini autorizzate da ordini giudiziari, rispettando i principi di necessità e proporzionalità e riducendo i falsi positivi.

Investire in tecnologie compatibili con la difesa della privacy, come la crittografia omomorfica[38], consentirebbe di analizzare dati cifrati senza decifrarli. La fully homomorphic encryption (FHE) supporta calcoli complessi, mentre la partially homomorphic encryption (PHE) è limitata a operazioni specifiche, con applicazioni

37. https://x.com/globalaffairs/status/1976638226132553768?s=46
38. vedi nota 7

in cloud computing, sanità e machine learning. Nonostante i limiti computazionali, queste tecnologie, insieme ai zero-knowledge proof. offrono soluzioni per rilevare contenuti illeciti senza violare l'E2EE, come sostenuto da oltre 500 scienziati[39].

Programmi di educazione digitale per giovani e famiglie, uniti a una cooperazione transnazionale con Europol e Interpol, rafforzerebbero poi la prevenzione e l'efficacia delle indagini.

Audit indipendenti e trasparenza algoritmica garantirebbero l'affidabilità delle tecnologie, mentre un dibattito pubblico inclusivo con cittadini, aziende e ONG eviterebbe approcci autoritari, favorendo soluzioni innovative. In conclusione, queste misure proteggono i minori, rispettano i diritti fondamentali e stimolano l'innovazione digitale europea.

8. Conclusioni

L'attuale proposta di chat control per come si rappresenta oggi, rappresenta una sfida cruciale. Pur perseguendo un obiettivo condivisibile, l'approccio basato sulla sorveglianza indiscriminata sembra incompatibile con i principi di necessità e proporzionalità del diritto europeo, violando tra le altre cose la riservatezza delle comunicazioni e il GDPR, e generando un potenziali forme di auto-censura da parte delle persone, intimorite dal rischio di essere intercettate.

Le tecnologie previste, come il client-side scanning, presentano rischi di falsi positivi, vulnerabilità di sicurezza ed eccessivi ampliamenti negli scopi della sorveglianza, minacciando la sicurezza digitale e l'affidabilità dei sistemi.

Economicamente, la proposta rischia di spingere aziende come Signal fuori dall'UE, con perdite per il settore tecnologico e una potenziale riduzione degli investimenti in ricerca e sviluppo.

Socialmente, la proposta erode la fiducia degli utenti, favorendo piattaforme non regolamentate. Mentre a livello globale, potrebbe ulteriormente legittimare pratiche di sorveglianza autoritarie, minando la privacy e l'innovazione in ambito democratico.

Le big tech, da WhatsApp a Signal, passando per Telegram e X (ex Twitter), si oppongono alla scansione delle comunicazioni cifrate.

In questo contesto, è fondamentale ribadire che la riservatezza della corrispondenza, anche in forma digitale, rappresenta, prima ancora che una questione tecnica, giuridica o politica, una condizione essenziale per l'esercizio di numerosi diritti fondamentali. Essa costituisce uno degli elementi imprescindibili della dignità della persona, come riconosciuto dall'articolo 1 della Carta dei Diritti Fondamentali dell'Unione Europea. Il suo riconoscimento come diritto costituzionalmente garantito nasce proprio dalla necessità di proteggere i cittadini da interferenze indebite da parte dello Stato, indipendentemente dalle ragioni che possono essere invocate, anche quando motivate da esigenze di ordine o sicurezza pubblica. Qualunque forma di compromissione, anche lieve, finisce per minare le basi dello Stato di diritto, già sotto pressione ovunque, anche in molti contesti democratici

39. https://www.patrick-breyer.de/en/danger-to-democracy-500-top-scientists-urge-eu-governments-to-reject-technically-infeasible-chat-control/

contemporanei.

Questa analisi propone quindi un approccio alternativo, basato su indagini giudiziarie, crittografia omomorfica, educazione digitale, trasparenza e dialogo pubblico, che consentirebbe di combattere il CSAM senza sacrificare i diritti fondamentali, stimolando un mercato di investimenti in tecnologie digitali stimato in crescita entro il 2030.

Il voto previsto - e poi slittato - per il 14 ottobre 2025 avrebbe rappresentato un momento importante: un'occasione per respingere l'attuale proposta, promuovere soluzioni più equilibrate e rafforzare la mobilitazione pubblica.

Se il voto si fosse svolto e la proposta fosse stata approvata, si sarebbe avviata la fase successiva di negoziazione tra Parlamento e Consiglio.

Tuttavia, a causa dell'incompatibilità di posizioni tra gli Stati membri, il voto è stato rinviato.

Non sappiamo con certezza quando la proposta tornerà all'ordine del giorno. È possibile ipotizzare che la prossima discussione sulla proposta possa avere luogo il 6 o 7 dicembre prossimi, in occasione della nuova riunione dei ministri degli Interni dell'UE.

È chiaro però che la presidenza danese non potrà ripresentare la proposta nella sua forma attuale: sarà necessario elaborare una versione modificata.

In questa prospettiva, è necessario riflettere sulla questione nell'ottica di preservare un Internet libero, sicuro, democratico e capace di promuovere l'innovazione.

ISTITUTO BRUNO LEONI
IDEE PER IL LIBERO MERCATO

IBL Focus

Chi Siamo

L'Istituto Bruno Leoni (IBL), intitolato al grande giurista e filosofo torinese, nasce con l'ambizione di stimolare il dibattito pubblico, in Italia, promuovendo in modo puntuale e rigoroso un punto di vista autenticamente liberale. L'IBL intende studiare, promuovere e diffondere gli ideali del mercato, della proprietà privata, e della libertà di scambio. Attraverso la pubblicazione di libri (sia di taglio accademico, sia divulgativi), l'organizzazione di convegni, la diffusione di articoli sulla stampa nazionale e internazionale, l'elaborazione di brevi studi e briefing papers, l'IBL mira ad orientare il processo decisionale, ad informare al meglio la pubblica opinione, a crescere una nuova generazione di intellettuali e studiosi sensibili alle ragioni della libertà.

Cosa Vogliamo

La nostra filosofia è conosciuta sotto molte etichette: "liberale", "liberista", "individualista", "libertaria". I nomi non contano. Ciò che importa è che a orientare la nostra azione è la fedeltà a quello che Lord Acton ha definito "il fine politico supremo": la libertà individuale. In un'epoca nella quale i nemici della libertà sembrano acquistare nuovo vigore, l'IBL vuole promuovere le ragioni della libertà attraverso studi e ricerche puntuali e rigorosi, ma al contempo scevri da ogni tecnicismo.

Istituto Bruno Leoni – Piazza Cavour 3 - 10123 Torino – Italy
T: +39 (011) 1978 1215 – F: +39 (011) 1978 1216 – www.brunoleoni.it – info@brunoleoni.it