

# **Chat Control 2.0: il punto di non ritorno della sorveglianza digitale europea**

Chat Control 2.0 rappresenta il più ambizioso progetto di sorveglianza digitale mai proposto in Europa: un regolamento che autorizzerebbe la scansione automatica di messaggi, email e contenuti privati di centinaia di milioni di cittadini. L'obiettivo dichiarato è contrastare la pedopornografia online, ma il prezzo da pagare potrebbe essere la fine della segretezza delle comunicazioni. Con l'avvio dei triloghi a dicembre 2025, l'UE si trova a un bivio tra sicurezza e libertà fondamentali.

## **Perché l'astensione dell'Italia potrebbe trasformarsi in un diniego costituzionale al regolamento**

Chat Control è una proposta della Commissione Europea che prevede l'introduzione di sistemi automatizzati in grado di scansionare messaggi, immagini e video privati alla ricerca di contenuti illegali relativi allo sfruttamento dei minori. La misura si applicherebbe potenzialmente a:

- chat private (WhatsApp, Signal, Telegram, Messenger, ecc.);
- email;
- servizi cloud;
- piattaforme di gaming con messaggistica integrata;
- strumenti di comunicazione interna nelle aziende;
- backup personali.

Una delle caratteristiche più criticate della proposta è che la scansione avverrebbe anche in assenza di un sospetto, configurando una forma di sorveglianza generalizzata e preventiva, senza distinzione tra cittadini innocenti e criminali.

L'obiettivo dichiarato è nobile e incontestabile: contrastare la pedopornografia online, un fenomeno odioso e in crescita. Tuttavia, la strada scelta dall'Unione Europea apre scenari delicatissimi per la privacy, la sicurezza digitale e, in ultima analisi, la tenuta democratica del continente.

La fase finale dei negoziati tra Parlamento Europeo, Commissione e Consiglio (trilogo) è iniziata il 9 dicembre 2025. Se non ci saranno impedimenti, Chat Control potrebbe diventare effettivo tra marzo e aprile 2026.

L'avvio del trilogo rappresenta molto più della fase conclusiva di un iter legislativo: è il momento in cui l'UE decide se costruire o meno la più grande infrastruttura di sorveglianza preventiva della storia democratica europea.

L'astensione dell'Italia, insieme a quella della Germania, non è un dettaglio politico. È un segnale d'allerta: molti elementi del regolamento appaiono in contrasto con i principi costituzionali degli Stati membri, in particolare con l'articolo 15 della Costituzione italiana, che garantisce l'inviolabilità della libertà e della segretezza delle comunicazioni. Non è un tecnicismo giuridico, ma il cuore del rapporto tra individuo e potere pubblico.

## **Il paradosso strutturale di Chat Control 2.0: una sorveglianza preventiva, non reattiva**

Il regolamento nasce per contrastare gli abusi sessuali sui minori online, obiettivo che nessuno contesta. Ma la modalità scelta rappresenta un cambio di paradigma: dalla sorveglianza mirata, basata su indizi concreti e autorizzata da un giudice, alla sorveglianza preventiva, generalizzata e algoritmica su tutta la popolazione.

Una svolta che ricorda il passaggio dal "controllo su indizi" al "profiling predittivo" tipico dell'intelligence, applicato

però al cuore della vita digitale: le comunicazioni private.

## **Il falso mito della “volontarietà” e il meccanismo di pressione normativa**

La prima bozza (bocciata il 9 ottobre 2025) prevedeva esplicitamente la scansione generalizzata dei contenuti delle chat, comprese quelle protette da crittografia end-to-end. Non sorprende che le critiche siano arrivate da EDPS, Garanti nazionali, esperti di sicurezza, giuristi e attivisti per i diritti digitali, che la consideravano una forma di sorveglianza di massa incompatibile con i principi europei.

La versione riscritta dalla Danimarca modifica l'impianto originario. Secondo il mandato negoziale approvato dal Consiglio, la rilevazione diventa formalmente volontaria: i gestori dei servizi possono scegliere se applicarla o meno. Il nuovo impianto prevede che:

- i provider possano scegliere se attivare la scansione;
- debbano comunque effettuare una valutazione obbligatoria del rischio;
- se risultano “ad alto rischio”, le autorità possano imporre misure correttive;
- sul piano economico e reputazionale, la scelta più sicura diventa attivare la scansione.

È un classico caso di *compliance indotta*: la legge non ordina esplicitamente, ma rende troppo rischioso non conformarsi. Per questo gli analisti definiscono la scansione “volontaria” solo sulla carta ma coercitiva nella sostanza.

La scelta non spetta agli utenti, ma ai provider: sono loro a decidere se i nostri messaggi saranno analizzati.

C'è poi un ulteriore incentivo: più comunicazioni vengono scansionate, più dati possono essere usati per addestrare modelli di intelligenza artificiale. Un vantaggio economico e tecnologico che può spingere verso una sorveglianza

permanente.

La storia recente suggerisce che la distinzione tra obbligo formale e pressione informale è spesso teorica, durante la pandemia, molte piattaforme hanno rimosso o penalizzato contenuti su pressioni politiche, come rivelato dai Twitter Files e dalle dichiarazioni di Mark Zuckerberg al Congresso USA, il risultato è stato un ecosistema di censura di fatto su contenuti perfettamente leciti, etichettati come disinformazione o “lawful but awful”, tecnicamente legali ma politicamente scomodi. Ciò che era “volontario” si è trasformato in uno standard di fatto. Applicata a Chat Control, la dinamica diventa particolarmente pericolosa.

## **Una tensione giuridica irrisolta: privacy e sicurezza in conflitto strutturale**

Il regolamento promette che la crittografia end-to-end non verrà indebolita. Ma per rilevare contenuti illeciti in una comunicazione cifrata, l'unico punto di intervento è il dispositivo dell'utente, prima della cifratura, cioè il client-side scanning, tecnicamente equivalente ad una intercettazione generalizzata.

La vera spia di allarme rosso su cui riflettere, è nell'articolo 85(1a) della bozza di regolamento, che incarica la Commissione di valutare periodicamente tecnologie di rilevazione per servizi con crittografia E2EE. Oggi non possono imporre il client-side scanning, ma si riservano il diritto di riprovarci.

La domanda diventa inevitabile: se ogni messaggio può essere analizzato prima di essere cifrato, la comunicazione è ancora “segreta” ai sensi dell'articolo 15 della Costituzione? Molti giuristi rispondono NO.

Da qui la possibile trasformazione dell'astensione italiana in un diniego costituzionale: l'ordinamento non può approvare una norma che svuota di fatto la segretezza delle comunicazioni

per 60 milioni di cittadini.

## **Function creep: un'infrastruttura pronta per usi futuri**

Il regolamento delinea un apparato completo:

- un EU Centre con database, indicatori e metriche;
- comitati tecnici incaricati di sviluppare ulteriormente tecnologie di mitigazione;
- obblighi per i provider di integrare strumenti di rilevazione quando richiesto.

Oggi il focus è il CSAM. Domani potrebbe essere terrorismo, hate speech, disinformazione, opposizione politica “radicale”. Una volta costruita l'infrastruttura, ampliarne lo scopo sarà una decisione politica, non tecnica. È il rischio classico di *function creep*, che in un contesto democratico dovrebbe essere considerato inaccettabile.

## **L'EU Centre: un nuovo potere sovranazionale con capacità operative ibride**

L'EU Centre on Child Sexual Abuse:

- riceve segnalazioni da provider e piattaforme
  - le valida con algoritmi e revisori umani
  - coopera direttamente con le forze dell'ordine
  - può influenzare tecnologie e standard europei sulle comunicazioni private

Nasce così una struttura sovranazionale, non eletta, con poteri operativi, tecnici e normativi. È esattamente il contesto in cui il *function creep* diventa più probabile: una volta installato un sistema di sorveglianza generalizzata, impedirne l'estensione è quasi impossibile.

# **Il rischio strategico: la normalizzazione della sorveglianza algoritmica in Europa**

La tecnologia raramente rimane confinata allo scopo originario.

Se esiste un'infrastruttura capace di analizzare contenuti, identificare pattern, coordinare polizie, profilare rischi, la tentazione di estenderla sarà inevitabile.

Storicamente, il passaggio dall'abuso sui minori al dissenso politico è il più documentato nello sviluppo dei sistemi di sorveglianza.

## **Proporzionalità e necessità: due principi europei ignorati**

La Corte di Giustizia dell'UE ha stabilito in più sentenze (Digital Rights Ireland, Tele2 Sverige, La Quadrature du Net) che:

- la sorveglianza generalizzata delle comunicazioni non è mai proporzionale;
- è ammessa solo su individui o gruppi specifici;
- la raccolta preventiva e indiscriminata viola la Carta dei Diritti Fondamentali.

Chat Control 2.0 entra pienamente in questo schema vietato. Come potrà superare il vaglio della Corte una volta approvato?

## **La vulnerabilità sistemica della società digitale europea**

Creare un meccanismo di scansione centralizzato significa:

- aumentare la superficie d'attacco per spionaggio e cybercrime;
- introdurre backdoor potenziali nelle piattaforme;
- facilitare abusi interni;

- indebolire l'ecosistema della crittografia.

Qualsiasi infrastruttura progettata per “controllare tutto” diventa un bersaglio irresistibile per Stati ostili e cybercriminali. Una vulnerabilità in un tale sistema comporta rischi sistemici per milioni di cittadini.

## **L'effettività: il regolamento colpisce davvero i criminali?**

Gli abusi reali vengono spesso scambiati:

- in darknet chiuse;
- su reti P2P cifrate;
- tramite strumenti decentralizzati;
- in circoli privati offline;
- in contesti che il regolamento non può raggiungere.

Chat Control rischia dunque di colpire soprattutto i cittadini comuni, lasciando intatti i criminali più organizzati, producendo falsi positivi e sovraccaricando le indagini.

## **Falsi positivi e “danno collaterale digitale”**

Il regolamento riconosce formalmente l'esistenza degli errori, citando falsi positivi, falsi negativi, oversight umano e metriche di errore.



Tabella 1

Dalla Tabella 1 emergono elementi strutturali inquietanti :

## **Gli errori sono considerati inevitabili**

Il testo richiede tecnologie “sufficientemente affidabili”, invita a “limitare al massimo possibile il tasso di errori” e prevede valutazioni periodiche, ma:

- non esistono soglie minime di accuratezza;
- non esistono limiti oltre i quali la tecnologia è vietata;

- non esistono criteri chiari per definire l'accettabilità dell'errore.

L'errore, però, non è neutrale: significa cittadini innocenti che finiscono in database, sotto indagine o con account sospesi.

## **“Limitare al massimo possibile”: una formula vaga**

Chi decide qual è “il massimo possibile”? Quali benchmark? Con quali sanzioni in caso di imprecisione?

Il rischio è che la formula diventi un paracadute retorico per giustificare sistemi con numerosi falsi positivi.

## **Oversight umano: paracadute o illusione?**

Il regolamento insiste su “oversight umano regolare”, ma nella pratica:

i volumi saranno altissimi;  
il lavoro è psicologicamente gravoso;  
la pressione regolatoria spinge al “meglio segnalare troppo”.

Il controllo umano può trasformarsi in un clic routinario.

## **Metriche per le autorità, opacità per gli utenti**

L'articolo 83 impone metriche ai provider, ma:

- solo EU Centre e autorità vedono i dati;
- gli utenti non hanno accesso a statistiche dettagliate;
- manca trasparenza granulare.

Lo Stato può normalizzare statisticamente l'errore; chi vi finisce dentro lo vive come una violazione gravissima.

## **Incentivo all'over-reporting**

Segnalare troppo poco comporta rischi; segnalare troppo non comporta costi. Il sistema è strutturalmente orientato all'eccesso di segnalazione.

## **Tutela ex post, danno ex ante**

Il regolamento prevede:

- reclami;
- ricorsi;
- rappresentanza tramite enti.

Ma quando l'utente agisce:

- il contenuto è già stato rimosso;
- l'account può essere sospeso;
- la segnalazione è già arrivata alle autorità;
- un'indagine può essere iniziata.

Anche in caso di archiviazione restano log, copie, danni emotivi e reputazionali. È un modello "ti proteggerò dopo averti colpito". Nel complesso, il regolamento appare costruito per accettare l'errore come costo sistemico, confidando che metriche e oversight lo mantengano gestibile.

## **Asimmetria informativa e crisi di fiducia**

Le autorità vedono tutto in macro; i provider controllano l'infrastruttura; i cittadini vedono solo gli effetti sul proprio account. Questo si inserisce in un contesto europeo già segnato dal crollo di fiducia verso istituzioni, media e organismi sovranazionali.

In tale scenario, Chat Control può essere percepito:

- come strumento di ordine in un mondo instabile;
- come strumento di sorveglianza contro dissidenti, giornalisti e oppositori.

Più la fiducia cala, più cresce la tentazione dei governi di usare il controllo al posto del consenso.

E più cresce il controllo, più la fiducia cala: un circolo vizioso.

# **Guerra, intelligence e libertà: un equilibrio fragile**

L'Europa si sta riarmando come non accadeva da decenni, in un contesto di confronto ibrido con la Russia e di instabilità globale. In scenari del genere, la privacy tende a diventare un ostacolo operativo.

La storia lo dimostra: dopo l'11 settembre, il Patriot Act ha compresso diritti che, vent'anni dopo, sono ancora lì. Il rischio è che Chat Control diventi il primo pezzo di un'architettura permanente di sorveglianza digitale, giustificata dalla protezione dei minori ma pronta a espandersi ad altre emergenze future.

## **Perché l'Italia potrebbe dire definitivamente “no”: l'argomento costituzionale**

Nessuna legge, nemmeno europea, può introdurre un sistema generalizzato di controllo delle comunicazioni in contrasto con l'articolo 15 della Costituzione.

L'unica eccezione ammessa richiede:

- un'indagine specifica;
- un atto motivato dell'autorità giudiziaria;
- destinatari determinati.

Chat Control 2.0 viola tutti e tre questi criteri. L'Italia deve quindi scegliere tra approvare un regolamento anticostituzionale o porre un diniego formale, avviando un conflitto giuridico con Bruxelles. L'astensione è un messaggio: l'Italia non può accettare un regolamento che viola un diritto “inviolabile”.

## **La questione politica più ampia: quale modello di società digitale vuole l'Europa?**

Chat Control 2.0 non è solo un tema tecnico. È una scelta di civiltà.

Si delineano due modelli:

- **Sicurezza preventiva attraverso sorveglianza pervasiva**  
Simile ai modelli cinesi, russi o a quelli post-11 settembre.
- **Tutela dei diritti fondamentali come limite al potere**  
Tradizione europea basata su proporzionalità, necessità, segretezza delle comunicazioni, warrant giudiziario, presunzione di innocenza.

Con Chat Control l'UE rischia di abbandonare gradualmente il secondo modello per avvicinarsi al primo.

## **Una società che rinuncia alla privacy rinuncia alla democrazia**

La privacy non è un lusso: è la condizione che consente a giornalisti, attivisti, dissidenti e cittadini di operare senza paura. La sorveglianza preventiva produce autocensura sistemica e modifica i comportamenti umani prima ancora dell'intervento repressivo.

## **Chat Control 2.0 è una scelta antropologica, non tecnica**

La questione è semplice, radicale, si basa su queste domande: Siamo disposti ad accettare una società in cui ogni comunicazione può essere analizzata da algoritmi? Siamo pronti a sacrificare la segretezza delle comunicazioni sulla promessa di tecnologie che generano errori elevati? Siamo consapevoli che i criminali continueranno a operare su canali invisibili mentre il controllo ricadrà sui cittadini comuni?

L'Italia, con il suo quadro costituzionale, ha la responsabilità di sollevare queste domande. Una volta costruita un'infrastruttura di sorveglianza generalizzata, smantellarla sarà quasi impossibile. Il 9 dicembre 2025 rischia di essere ricordato non come il giorno in cui l'Europa ha difeso i minori, ma come il giorno in cui ha aperto la

porta alla più grande infrastruttura di sorveglianza mai approvata in tempo di pace. Per chi si occupa di democrazia, diritto e cybersicurezza, la posta in gioco è altissima: superata la linea della segretezza delle comunicazioni, tornare indietro sarà quasi impossibile.

#### Profilo Autore



Progettista di sistemi esperti, software developer, network e system engineer, con oltre 30 anni di esperienza nell'ambito della sicurezza delle informazioni, Francesco Arruzzoli è il Resp. del Centro Studi Cyber Defense Cerbeyra, dove svolge attività di R&D, analisi delle cyber minacce e progettazione di nuove soluzioni per la cyber security di aziende ed enti governativi. Esperto di Cyber Threat Intelligence e contromisure digitali, autore di libri ed articoli sue riviste del settore, in passato ha lavorato per multinazionali, aziende della sanità italiana, collaborato con enti governativi e militari. In qualità di esperto cyber ha svolto inoltre attività di docenza presso alcune università italiane.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/chat-control-2-0-sorveglianza/>