

Chat Control 2.0, gli esiti incerti della contestata proposta di regolamento europeo



Lunedì 29 giugno l'Unione Europea è tornata a discutere del Regolamento 2022/0155 CSAR (*Child Sexual Abuse Regulation*), più noto come **“Chat Control 2.0”**.

Presentato nel 2022, negli anni il testo è stato oggetto di numerosi *round* negoziali tra Parlamento, Consiglio e Commissione UE; allo stesso tempo è finito al centro di accese critiche legate al rischio di avallare forme di sorveglianza digitale sugli utenti.

Per meglio inquadrare l'esito dell'incontro, nel presente articolo ripercorriamo l'*iter* normativo, i contenuti e le principali criticità della proposta di regolamento.

L'iter della proposta CSAR

Il passaggio iniziale risale all'11 maggio 2022, quando la Commissione Europea annunciò di voler introdurre un regolamento mirato a *“prevenire e combattere l'abuso sessuale sui minori”*.

Alla luce dell'evoluzione delle tecnologie e del mutato panorama di rischio, la proposta si affiancava alla precedente Direttiva 2011/93 e abrogava il Regolamento 2021/1232 – noto come **“Chat Control 1.0”** – che prevedeva una deroga temporanea alla direttiva ePrivacy del 2002, per consentire agli erogatori dei servizi digitali la scansione volontaria delle conversazioni sulle proprie piattaforme a fini di rilevazione

e rimozione del *Child Sexual Abuse Material* (CSAM).

La nuova formulazione assegnava ai gestori dei servizi un ruolo più stringente, prevedendo uno *scanning* non più volontario ed episodico ma preventivo e massivo, allo scopo di contrastare più efficacemente lo CSAM e i fenomeni di *grooming*.

Negli anni seguenti, tuttavia, diversi pareri e relazioni tecniche degli organi comunitari avrebbero evidenziato le possibili insidie di simili ingerenze nelle comunicazioni private dei cittadini.

Nonostante tali criticità, inizialmente gran parte degli Stati membri annunciò il proprio favore per l'adozione della normativa; ma in seguito si diffusero crescenti dubbi verso le misure proposte, tanto che le consultazioni avvenute nell'ottobre 2025 terminarono con esito negativo (mentre il 26 novembre il Consiglio avrebbe poi raggiunto una posizione comune).

Dopo una parziale revisione del testo, svoltasi sotto la Presidenza danese del Consiglio UE, alla fine del 2025 si è quindi aperto un processo negoziale – tuttora in corso – che ha coinvolto Parlamento, Consiglio e Commissione europea.

L'*iter* ha registrato un'evoluzione fondamentale a marzo, quando la Commissione Giustizia, Libertà civili e Affari interni (LIBE) ha respinto la deroga provvisoria alla direttiva ePrivacy con 28 voti favorevoli e 38 contrari; pochi giorni dopo, anche il Parlamento si sarebbe pronunciato a sfavore, portando alla scadenza della proroga il 3 aprile 2026.

Il nodo della crittografia *end-to-*

end

Uno dei principali nodi critici della proposta risiede nella previsione di una sorveglianza preventiva generalizzata, che permetterebbe alle aziende *tech* di accedere a chat di messaggistica ed email di milioni di persone senza necessità di alcun controllo giudiziario, così violando il principio di riservatezza della vita privata sancito dall'art. 8 della Convenzione Europea sui Diritti Umani (CEDU).

Questo richiederebbe di verificare i messaggi mediante il *client-side scanning*, analizzando i contenuti direttamente sul dispositivo dell'utente prima di applicare la crittografia *end-to-end* (E2E); ne deriverebbero serie implicazioni anche per le aziende responsabili dei servizi, costrette a monitorare costantemente i contenuti condivisi dai propri utenti alla ricerca di materiali illeciti.

È ovvio che l'unico modo per garantire tale monitoraggio su un'immensa mole di conversazioni sarebbe implementare forme di scansione automatizzata delegate a sistemi basati sull'AI, con quanto ne consegue in termini di falsi positivi ed errori dagli effetti potenzialmente molto gravi per la vita e la reputazione dei cittadini coinvolti, come del resto aveva rilevato sin da subito il parere congiunto EDPB–EDPS n. 4/2022.

Anche l'imposizione di meccanismi di *age verification* avrebbe serie conseguenze in termini di identificazione e profilazione degli utenti, portando a una sostanziale cancellazione del diritto all'anonimato online.

Soprattutto, minare la crittografia *end-to-end* significherebbe esporre a seri pericoli gruppi di persone già particolarmente vulnerabili alla sorveglianza digitale: come giornalisti investigativi, oppositori politici e perfino vittime di *cyber stalking*, che non potrebbero più contare su alcuna garanzia circa la segretezza delle proprie comunicazioni online.

Gli attuali contenuti: “Chat Control 2.0”

Allo scopo dichiarato di proteggere i minori da ogni forma di abuso, il testo del regolamento abilita il *mass scanning* preventivo sulle email e i messaggi privati dei cittadini, rischiando di fatto di introdurre forme di sorveglianza digitale generalizzata sugli utenti europei.

Dopo la revisione avvenuta alla fine del 2025 si è tornati a parlare, come già nel Chat Control 1.0, di “scansione volontaria” e non obbligatoria; tuttavia, si continuano a prevedere misure obbligatorie di *risk assessment* (Art. 3) e *risk mitigation* (Art. 4) a carico delle aziende erogatrici di servizi di comunicazione digitale.

Si sancisce poi l’obbligo di introdurre meccanismi di verifica dell’età per i servizi di *hosting* e comunicazione, richiedendo l’esibizione di un documento d’identità o l’utilizzo di credenziali biometriche per accedere a servizi e piattaforme online.

Nel regolamento viene infine anticipata la costituzione di un nuovo centro di controllo europeo incaricato di coordinare le attività di prevenzione e contrasto della violenza sui minori, con cui le aziende tecnologiche saranno tenute a collaborare attivamente.

La posizione dell’Italia sul Regolamento

Inizialmente tra i sostenitori della proposta, negli ultimi due anni l’Italia ha progressivamente sfumato la propria posizione sul regolamento CSAR.

Tuttavia, pur continuando a dichiararsi contraria alla previsione di forme di scansione massiva sulle comunicazioni

private, nel Coreper di novembre il nostro Paese ha scelto non di esprimere un voto contrario ma di astenersi, come ha fatto anche la Germania.

Una scelta ambigua, che lascia aperte numerose domande sulla reale posizione del governo circa una normativa che potrebbe impattare profondamente la privacy dei propri cittadini.

Le iniziative della società civile

Com'era prevedibile, nei quasi cinque anni trascorsi dalla sua proposizione il Regolamento non è rimasto esente da valutazioni negative.

Le più accese provengono dalle associazioni per i diritti digitali, le quali hanno lanciato una petizione contro l'approvazione della normativa, evidenziando che prevedere una scansione generalizzata su email e servizi di messaggistica equivale a sancire la fine della privacy come concepita in seno all'Unione Europea.

Anche numerosi esperti di cybersecurity si sono pronunciati contro la proposta, ricordando come sancire l'aggirabilità della crittografia E2E significhi, tra le altre cose, aprire la porta ad ogni tipo di vulnerabilità sui dispositivi degli utenti.

E se i proponenti parlano di un "vuoto normativo" da colmare con urgenza, gli oppositori continuano a ricordare che esistono altre strade per combattere un fenomeno odioso come lo CSAM, senza necessariamente imporre a milioni di cittadini incolpevoli di rinunciare alla privacy delle loro comunicazioni digitali.

Gli esiti dell'incontro del 29

giugno

Qualora nel trilogico di lunedì 29 giugno 2026 fosse stato raggiunto un accordo, l'adozione formale del regolamento CSAR sarebbe probabilmente arrivata entro la fine di luglio.

L'incontro non ha invece saputo individuare una posizione comune su tutti i punti in discussione, avendo come esito un'ennesima proroga dei lavori.

Si conferma l'esistenza di un consenso diffuso rispetto alla maggior parte delle misure proposte, come le definizioni del fenomeno da contrastare o le funzioni del futuro Centro Europeo per la protezione dei Minori; restano tuttavia irrisolti gli aspetti relativi alla scansione automatica dei messaggi privati, da sempre il punto più contestato della normativa.

Intanto, secondo quanto riportano alcune fonti (italiane ed estere), il Coreper avrebbe nuovamente calendarizzato un incontro per procedere a revisionare la versione del regolamento in cui era prevista la scansione delle comunicazioni su base volontaria oggetto della proroga scaduta ad aprile, ossia il noto "Chat Control 1.0".

Ciò significherebbe aggirare la volontà espressa dal Parlamento per riproporre una proposta ormai definitivamente decaduta: di fatto una lesione senza precedenti ai meccanismi democratici comunitari, che – se confermata – non mancherà di suscitare nuove critiche e reazioni, ulteriormente complicando la già lunga e travagliata strada per l'approvazione del regolamento CSAR.

Condividi sui Social Network:

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