

Chat control

RIVOLUZIONE ONLINE – 15 LUGLIO 2026

Proteggere i bambini o sorvegliare tutti gli altri?

Il Parlamento europeo ha deciso, sfruttando un cavillo di procedura, che Gmail e Messenger possono leggere le nostre conversazioni: in automatico, prima che arrivino a destinazione e senza passare per un giudice. Se scatta un allarme, il caso va alla polizia. Apple fa lo stesso sui nostri telefoni, con foto e messaggi. Governi e piattaforme hanno gli stessi interessi in gioco: e la protezione dei minori non è tra questi.

Chat control

Da Bruxelles alla California

Giovedì il [Parlamento europeo](#) ha rimesso in piedi un permesso che consente a servizi come Gmail, Messenger o Skype di leggere il contenuto delle nostre conversazioni, per cercare materiale di abuso sui minori e tentativi di adescamento. Se lo trovano, lo segnalano a un'organizzazione che gira i casi alla polizia.

A marzo Bruxelles ne aveva bocciato la proroga, sembrava finita. Ma la presidente del Parlamento, [Metsola](#), ha chiesto al Consiglio di riproporla, e il suo partito ha ottenuto un voto d'urgenza l'ultimo giorno prima delle vacanze: per bloccarla serviva il no di 360 eurodeputati ma, con l'aula semivuota, quel numero fisso non è stato raggiunto. Ora il provvedimento va al Consiglio dell'Unione: la storia non è finita del tutto. Un negoziato parallelo, separato e più ambizioso, sta intanto definendo una versione permanente della stessa norma.

Un mese fa [Apple](#) ha presentato la nuova versione dei suoi sistemi operativi, con molto spazio dedicato ai bambini: account per minori e uno strumento che segnala i messaggi con foto non solo di nudo ma anche di violenza e sangue. Il controllo della foto lo fa il telefono stesso, in locale, ed ora anche altre app potranno integrarlo nel proprio prodotto. Funziona così: se lo strumento rileva qualcosa, sfoca l'immagine, avvisa il ragazzino, e se l'account è collegato a quello dei genitori può avvisare anche loro sul loro telefono. Qui il caso resta in famiglia: nessuna segnalazione alle autorità.

Il controllo preventivo di tutti i nostri messaggi

Apple e il Parlamento europeo stanno legittimando, ciascuno a modo suo (tra l'elaborazione locale a difesa del brand e la scansione centralizzata), e sotto la stessa bandiera della protezione dei minori, una capacità tecnica identica: **un sistema che legge, interpreta e giudica il contenuto di quello che scriviamo, prima ancora che arrivi a chi doveva riceverlo**. Quello che si sta costruendo, pezzo dopo pezzo, è l'infrastruttura che permetterebbe una sorveglianza molto più ampia di quella oggi realmente in uso: si costruisce proprio nel punto in cui nessuno oserebbe dire di no.

[Garanti della privacy](#) in Europa hanno esplicitamente avvertito che il rischio è di **arrivare a controllare, senza alcuna selezione, praticamente tutte le comunicazioni digitali degli europei**.

Dietro queste due notizie ci sono due tecnologie diverse: una consolidata da anni, una più recente e ancora in espansione.

La prima, **hashing**, è la più vecchia: in uso dal 2009 su email, cloud e social (Gmail, Facebook, Twitter, tra gli altri). Funziona come una impronta digitale: ogni immagine di abuso già segnalata diventa un codice unico, una firma. Se un file ha la stessa firma di uno già in lista nera, scatta la segnalazione. Un confronto meccanico, cieco al significato di quello che analizza: cerca solo quello che già conosce, per questo è relativamente sicuro.

La seconda, la **classificazione semantica**, è la tecnologia più recente, quella usata per riconoscere il *grooming*, l'adescamento: qui non c'è una firma da confrontare, perché quello da individuare è un comportamento, il modo in cui un adulto costruisce fiducia con un bambino messaggio dopo messaggio. Il sistema deve leggere le parole, valutare il tono, interpretare il contesto: deve capire il senso di quello che scriviamo, un compito molto più ambizioso del semplice confronto con una lista. Il suo perimetro non è fisso: si allarga o si restringe con un aggiornamento interno che nessuno può vedere fuori dall'azienda (Apple, Meta, ecc). E la stessa capacità di interpretare un testo può essere usata per altri controlli: per riconoscere l'adescamento, o per riconoscere chi critica un governo in una chat privata.

Un dato aiuta a capire le proporzioni: nel 2020 Facebook ha dichiarato che [oltre il 90% del materiale di abuso trovato sulla piattaforma era la copia di qualcosa già segnalato in passato](#) (ad esempio bastavano sei soli video, ripetuti in copie diverse, a spiegare più della metà di tutti i casi trovati quell'anno).

L'hashing, il sistema più semplice, cattura già da solo la gran parte del problema online. Per intercettare una piccola parte, dunque, ci stiamo giocando la nostra privacy.

Falsi positivi

A volte il sistema sbaglia. Nel 2021 [un padre in California](#) manda al pediatra, per una visita da remoto durante il covid, delle foto del figlio piccolo per un'infezione. Google le classifica come materiale di abuso: disattiva il suo account e segnala tutto alla polizia di San Francisco, che apre un'indagine durata mesi con accesso alla sua cronologia di ricerca, alla sua posizione, ai suoi messaggi. Lo scagionano: era solo un padre preoccupato. Google non gli ha mai restituito l'account.

Proteggere i bambini resta necessario. Ma chiediamoci se esiste un modo più mirato per arrivare allo stesso obiettivo e se la strada che stiamo prendendo, oltre a essere molto rischiosa per la violazione dei diritti, serve in realtà a tutt'altro che a proteggere i minori.

Chiediamoci ad esempio chi ci guadagna.

Le piattaforme

Senza il permesso che il Parlamento ha appena rinnovato, scansionare i messaggi violerebbe le regole europee sulla riservatezza, esponendo le aziende a cause legali. Con il permesso, le piattaforme possono farlo senza rischio, tutelando sia la propria immagine sia quel monitoraggio semantico dei contenuti che, in altri contesti, rappresenta la base della loro profilazione commerciale.

C'è poi un **mercato** vero dietro questi strumenti: le piattaforme comprano questi sistemi di riconoscimento da aziende specializzate che vendono lo stesso servizio a mezzo mondo, inclusi altri produttori di intelligenza artificiale ([Meta, Google, Microsoft, OpenAI e altri hanno aderito agli stessi standard di un fornitore specializzato](#)). Più ampia è la base legale che ne autorizza l'uso, più cresce quel mercato.

Ogni segnalazione generata da questi sistemi poi, prima di arrivare a un giudice o alla polizia, passa dentro il **software di un'azienda privata**: dal 2010 [chi elabora le segnalazioni di abuso per l'organizzazione americana che le raccoglie da tutto il mondo usa Palantir](#), la stessa azienda che lavora per intelligence e forze dell'ordine in mezzo mondo.

L'infrastruttura nata per proteggere i bambini finisce così per rafforzare un'azienda che ha già in mano pezzi importanti di funzioni che un tempo erano solo dello Stato.

I governi

Anche i governi hanno i loro interessi. A riportare in vita il permesso scaduto è stata soprattutto la presidente del Parlamento, che [a giugno ha scritto al Consiglio](#) chiedendogli di ripresentare un testo che l'aula aveva già bocciato. Un'iniziativa che ha risparmiato ai governi

il costo politico di apparire come chi rinvoca una norma sulla sorveglianza appena respinta.

Un vantaggio per la polizia: riceve segnalazioni già pronte, senza dover chiedere prima a un giudice di [autorizzare ogni controllo](#): obbligo che ha preso molti voti ma non è passato. Oggi, senza quel filtro, la scansione produce **piste investigative su chiunque, senza che serva prima un sospetto specifico su quella persona.**

La legge permanente, ancora in negoziato e distinta dal permesso appena rinnovato, prevede anche la **nascita di una nuova agenzia europea** dedicata proprio a questo tema, con un proprio budget e un proprio organico. Inoltre, la legge obbliga ogni azienda a [valutare il rischio del proprio servizio](#) e a ridurlo, pena multe fino al 6% del fatturato mondiale. Per ridurre quel rischio, dunque, le aziende **leggeranno i messaggi prima che vengano cifrati: un obbligo di fatto**, anche se la legge non lo chiama così. In questo modo i governi ottengono l'accesso ai contenuti cifrati senza doverlo imporre per legge.

Pedofilia e Internet: vecchie ossessioni e nuove crociate

Nel 1998, **agli albori del dibattito su Internet e pedofilia**, [Radio Radicale organizzò un convegno a Roma](#) per denunciare l'uso politico di quel binomio. Roberto **Cicciomessere** ricordava questo dato:

il 90% degli abusi sessuali sui minori avviene in famiglia, l'8% per mano di persone conosciute ma esterne alla famiglia, e solo il 2% per mano di sconosciuti.

Ventisette anni dopo, le statistiche internazionali raccolte da [RAINN](#) confermano la stessa proporzione: **il 93% delle vittime minorenni conosceva il proprio aggressore.**

Questo significa non solo che l'abuso online è una fetta piccola dell'abuso sui minori ma che già, come abbiamo visto, veniva colpito al 90% dallo strumento più semplice (**hashing**), quello delle impronte digitali.

È vero che l'adescamento online è cresciuto. Negli Stati Uniti le segnalazioni sono passate da [44.000 nel 2021 a oltre 1,4 milioni nel 2025](#), ma una parte di questa crescita dipende da una legge che ha reso obbligatoria la segnalazione. In parte dipende anche dalla definizione di materiale pedopornografico su Internet: in Pennsylvania l'ex governatore Corbett si è costruito una carriera politica sulla "protezione" dei minori. Peccato che la definizione di comportamento pedopornografico fosse così ampia che anche due fidanzatini di 17 anni che facevano sexting potevano ricadere nella definizione e ritrovarsi iscritti (a vita, senza appello) nella lista dei "sex offenders".

E resta un fatto scomodo per chi difende questi strumenti: è proprio la categoria dell'adescamento, quella che richiede la classificazione semantica, ad avere [secondo il Garante europeo della privacy i tassi di errore più alti](#) tra tutte le tecnologie di rilevamento.

I diritti dell'infanzia e dell'adolescenza

Tra scansionare tutto e non fare nulla ci sono alternative. Da anni, **organizzazioni per i diritti digitali e realtà per la protezione dell'infanzia**, [propongono misure diverse](#): rimuovere il materiale già individuato dalla rete invece di limitarsi a segnalarlo, finanziare meglio le unità di polizia specializzate che già indagano su questi reati, potenziare le linee di ascolto per le vittime gestite da personale formato al trauma, investire nell'educazione sessuale e digitale nelle scuole. In Italia, ad esempio, [un progetto di Save the Children e EDI Onlus](#) porta l'alfabetizzazione digitale in decine di scuole medie, con l'obiettivo dichiarato di rendere studentesse e studenti "utenti attivi, capaci non solo di usare gli strumenti digitali, ma anche di comprendere come funzionano e quale ruolo hanno nella società."

Sono misure che costano, in soldi e tempo, quello che il controllo automatico promette di risparmiare. La differenza è proprio questa: una **misura** come quella appena **approvata dal Parlamento non costa nulla ai governi e risolve forse solo una fetta piccola del problema reale.**

Ma risolve una grossa fetta di un altro problema reale: tra una scusa di pedofilia ed una minaccia di terrorismo, i governi si attrezzano a dispiegare una versione distopica del Panopticon di Bentham. **Il vero target è ovviamente il controllo, politico, economico e commerciale.** Non dimentichiamo lo scandalo che seguì la rivelazione del sistema Echelon: oltre a spiare i presunti terroristi (pochi per la verità, e con miserrimi risultati, viste le cronache), spiava le aziende europee a vantaggio dei concorrenti angloamericani, oltre ad [intercettare perfino le telefonate della Merkel.](#)

Le misure che chi lavora sul campo raccomanda da anni, quelle capaci di intercettare l'abuso dove avviene davvero, richiedono investimenti pubblici concreti. Consentire la scansione automatica costa un voto d'urgenza; finanziare una linea di ascolto o programmi di alfabetizzazione e sostegno costa un bilancio. Non è difficile capire quale, ai governi, convenga di più.

Non solo: un sistema pensato per proteggere un adolescente può finire per privarlo proprio dello **spazio privato di cui ha bisogno per chiedere aiuto**, anche quando quell'aiuto serve contro un adulto della sua stessa famiglia. Sapere di essere monitorati non rende i ragazzi più sinceri con i genitori, li rende più bravi a nascondersi.

Sul comportamento degli adolescenti online, un bellissimo studio sociologico di Diane Boyd intitolato ["It's complicated"](#) (parafrasando una delle possibili risposte nella definizione del profilo di Facebook alla voce "relationship"). La Boyd ha seguito un campione di ragazzi dai tempi di Myspace fino a Facebook e gli albori di Twitter. Le dinamiche online non sono mai cambiate.

In [uno studio su genitori che avevano ricevuto un avviso automatico su un rischio del proprio figlio](#), circa uno su quattro ha notato un **peggioramento della fiducia** dopo quell'avviso. Il filtro pensato per proteggere un adolescente rischia di essere proprio il motivo per cui smette di raccontare i propri problemi a un adulto.

Il conto che non torna

Stiamo costruendo un **sistema che leggerà preventivamente tutto quello che scriviamo, segnalerà alla polizia senza che serva prima un sospetto specifico su quella persona né il mandato di un giudice, e farà passare le segnalazioni nel software di un'azienda privata (Palantir) prima ancora che le veda un magistrato.**

È una tenaglia a due mani.

Da una parte i governi, che ottengono un'infrastruttura di controllo senza doverla imporre per legge (o addirittura, come in USA, in plateale contraddizione con le garanzie della Costituzione e pertanto in “esercizio provvisorio” di proroga in proroga sin dal 2001).

Dall'altra le piattaforme e chi vende loro questi strumenti, che ottengono copertura legale e un mercato in espansione.

A guadagnarci meno di tutti sono proprio i cittadini onesti. Visto il livello di automazione, un cittadino rischia un rinvio a **giudizio kafkiano per una serie di controlli automatici che scattano senza che nessuno possa intervenire.** Subire un processo è costoso, mangia il tempo, la vita, le relazioni e spesso anche se prosciolti, lascia danni permanenti su vita, lavoro, ecc. Cittadini sorvegliati su scala capillare per intercettare, come abbiamo visto, soprattutto materiale già noto: la parte più difficile da fermare, quella della produzione dell'abuso nel momento in cui accade, resta quasi sempre un fatto domestico, fuori dalla portata di qualunque sistema legga le nostre chat.

Una volta che questi meccanismi sono implementati, cosa impedisce ad un governo di chiedere ai fornitori di servizi e device di implementare una **censura su argomenti “non appropriati”**? O semplicemente di **“segnalarli” alle autorità**? O di **classificare i cittadini in base a orientamento politico, preferenze sessuali, allineamento con il governo**? Chi lo verrebbe a sapere? Chi potrebbe opporvisi?

Se il bersaglio dichiarato è davvero proteggere i minori, il conto non torna.

– di Paola Furlan e Andrea Mazzucchi