http://www.diva-portal.org

Postprint

This is the accepted version of a paper published in . This paper has been peer-reviewed but does not include the final publisher proof-corrections or journal pagination.

Citation for the original published paper (version of record):

Kelemen, K., Giaretta, A. (2026)
Chat Control e disallineamento tra diritto europeo e legislazione italiana sull'adescamento di minori
Questione Giustizia, (3): 302-310

Access to the published version may require subscription.

N.B. When citing this work, cite the original published paper.

Permanent link to this version:
http://urn.kb.se/resolve?urn=urn:nbn:se:oru:diva-130933

Chat Control e disallineamento tra diritto europeo e legislazione italiana sull'adescamento di minori*

di *Katalin Kelemen* e *Alberto Giaretta*

L'articolo analizza la proposta europea nota come "*Chat Control*" con specifico riferimento alla prevenzione e al rilevamento dell'adescamento di minori nelle comunicazioni digitali. Muovendo dall'esame del quadro normativo europeo e italiano, il contributo evidenzia un significativo disallineamento tra la definizione di «adescamento» accolta dalla Convenzione di Lanzarote e dalla direttiva 2011/93/UE, da un lato, e quella più ampia adottata dal legislatore italiano, dall'altro. Tale divergenza incide direttamente sulla compatibilità giuridica e sull'efficacia dei sistemi automatizzati di rilevazione previsti dalla proposta di regolamento. L'analisi mette in luce i limiti strutturali delle tecnologie di monitoraggio applicate alle comunicazioni testuali, il rischio di sovra- e sotto-inclusione delle condotte penalmente rilevanti e le conseguenti implicazioni per i diritti fondamentali, in particolare per la *privacy* e la certezza del diritto, auspicando un maggior coordinamento tra disciplina penale, soluzioni tecnologiche e obiettivi di armonizzazione europea.

1. Introduzione / 2. L'adescamento di minori nel diritto penale italiano / 3. I limiti strutturali del rilevamento dell'adescamento nelle comunicazioni private / 4. Il problema del disallineamento tra *Chat Control* e le norme europee / 5. Conclusione

1. Introduzione

La pandemia ha esposto i minori a un numero significativamente maggiore di approcci indesiderati *online*[1]. Di conseguenza, nel maggio 2022 la Commissaria europea per gli affari interni Ylva Johansson, esponente del Partito Socialdemocratico svedese, ha presentato una proposta di regolamento per la prevenzione e la lotta contro l'abuso sessuale su minori *online*[2]. La proposta, al centro di un dibattito con molti tentativi di revisione da allora, è diventata nota come "*Chat Control*" perché imporrebbe a tutti i prestatori di servizi di *hosting* e di comunicazione interpersonale di controllare i contenuti delle comunicazioni digitali, incluse quelle private, al fine di segnalare e contrastare la diffusione di materiale pedopornografico e i tentativi di adescamento di minori. La questione è tornata all'ordine del giorno nel 2025,

* Questo lavoro è stato sostenuto dal programma svedese «*Wallenberg AI, Autonomous Systems and Software Program – Humanities and Society*» (WASP-HS), finanziato dalla Fondazione Marianne e Marcus Wallenberg e dalla Fondazione Marcus e Amalia Wallenberg.

1. Interpol, *Threats and Trends Child Sexual Exploitation and Abuse: COVID-19 Impact*, settembre 2020 (www.interpol.int/en/content/download/15611/file/COVID19); K. Chauviré-Geib *et al.*, *The increase in online child sexual solicitation and abuse: Indicator 16.2.3 of the UN Sustainable Development Goals (SDG) documents a hidden and growing pandemic. Population-based surveys fail to capture the full picture*, in *Child Abuse & Neglect*, vol. 164, giugno 2025 (https://doi.org/10.1016/j.chiabu.2025.107452).

2. Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori*, COM (2022) 209 *final*, 11 maggio 2022 (https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52022PC0209).

con la presidenza danese del Consiglio dell'Unione europea. I negoziati stanno attualmente procedendo con alcune modifiche rispetto alla versione originale. Il compromesso, proposto dal Ministro della giustizia danese Peter Hummelgaard, è quello di mantenere l'attuale sistema di monitoraggio volontario, in vigore fino ad aprile 2026, anziché renderlo obbligatorio, al fine di non perdere uno strumento importante nella lotta contro gli abusi sessuali sui minori[3].

La proposta si basa su alcune osservazioni cardine. La prima osservazione è che la quantità di dati disponibili *online* è troppo estesa per poter essere analizzata da operatori umani. La seconda, e forse più importante, osservazione è che parte di questi crimini avviene tramite interazione diretta con le vittime, e la crittografia *end-to-end* non consente ai prestatori di servizi di accedere in alcun modo a tali dati. L'utilizzo di strumenti automatici basati sull'intelligenza artificiale porta a risultati significativamente migliori per quanto concerne l'identificazione di materiale pedopornografico[4]. Inoltre, non è possibile fare affidamento esclusivamente sulle segnalazioni degli utenti, poiché tali segnalazioni mostrano un'alta percentuale di falsi positivi. Uno studio dell'*Internet Watch Foundation* condotto nel 2023 ha mostrato che soltanto il 34% delle segnalazioni di materiale relativo ad abusi sessuali su minori ricevute dal pubblico si è rivelato pertinente[5].

Chat Control è stata oggetto di critiche accese da molteplici parti, sia dalla comunità giuridica che da quella tecnologica[6]. I critici sostengono che il monitoraggio delle comunicazioni private comprometterebbe la *privacy* e la cifratura, creando strumenti che potrebbero essere riutilizzati per altri tipi di controllo. Al contempo, come osservato anche dal Comitato europeo per la protezione dei dati (EDPB) e dal Garante europeo della protezione dei dati (GEPD), non sembra attualmente sussistere alcuna soluzione tecnologica in grado di rilevare materiale pedopornografico condiviso in forma cifrata; pertanto, le misure di rilevazione previste dalla proposta potrebbero avere un impatto inferiore a quello auspicato[7]. Inoltre, per quanto riguarda la rilevazione dell'adescamento di minori nelle comunicazioni sotto forma di testo, le tecnologie esistenti presentano un tasso di accuratezza inferiore rispetto ai risultati ottenuti con materiale fotografico[8]. Per questi motivi, e per il drastico abbassamento della soglia di punibilità del reato di adescamento di minori da parte del legislatore italiano rispetto alle linee guida degli strumenti internazionali, come spiegato in seguito, il presente articolo si limita a esaminare le problematiche che emergono in relazione all'applicazione della proposta *Chat Control* per la rivelazione dell'adescamento di minori *online*.

2. L'adescamento di minori nel diritto penale italiano

Il reato di «adescamento di minorenni» è stato introdotto nell'ordinamento italiano nel 2012 per dare attuazione alla cd. Convenzione di Lanzarote,

3. *Hummelgaard opgiver kontroversielt forslag om overvågning*, *Politiken*, 30 ottobre 2025 (https://politiken.dk/viden/art10605607/Hummelgaard-opgiver-kontroversielt-forslag-om-overvågning); V. Alvich, *Chat Control, stop definitivo alla (controversa) proposta di legge europea per la lotta alla pedopornografia*, *Corriere della Sera*, 25 novembre 2025 (www.corriere.it/tecnologia/25_novembre_03/chat-control-stop-definitivo-alla-controversa-proposta-di-legge-europea-per-la-lotta-alla-pedopornografia-c747d2af-1aaa-42b8-86f3-b291a58e9xlk.shtml).

4. "*PhotoDNA*" di *Microsoft*, usato da più di 150 organizzazioni nel mondo per identificare materiale pedopornografico noto con la tecnologia di "*hashing*", ha un alto tasso di accuratezza. Il tasso di falsi positivi è stimato in non più di 1 su 50 miliardi. Altri strumenti simili che usano la stessa tecnologia sono "*CSAI Match*" di *YouTube* e "*PDQ*" di *Facebook*. Per l'individuazione di nuovo materiale pedopornografico sono, invece, usati classificatori e altre tecnologie di intelligenza artificiale, ad esempio "*Safer*" di *Thorn*. Vds. Commissione europea, *Impact Assessment Report Accompanying the document "Proposal for a Regulation of the European Parliament and of the Council laying down rules to revent and combat child sexual abuse"*, SWD (2022) 209 *final*, 11 maggio 2022, *Annex* 8, pp. 281-282 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0209).

5. Nel 2023, la Hotline dell'IWF ha valutato 132.710 segnalazioni provenienti dal pubblico: vds. Internet Watch Foundation, *Annual Report 2023* (www.iwf.org.uk/annual-report-2023/?back=true).

6. EDPB-GEPD, *Parere congiunto n. 4/2022 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori*, 28 luglio 2022; Clusit (Associazione italiana per la sicurezza informatica; https://clusit.it/chi-siamo/), *Serve prudenza su Chat Control*, 3 novembre 2025 (https://clusit.it/wp-content/uploads/area_stampa/2025/Clusit_CSAR.pdf); M. Schiaffino, *Fermate Chat Control! Il grido d'allarme di attivisti ed esperti di privacy*, *Wired*, 2 ottobre 2025 (www.wired.it/article/chat-control-grido-allarme-attivisti-privacy/).

7. EDPB-GEPD, *Parere congiunto n. 4/2022*, *cit.*, n. 6, par. 45.

8. Nel 2022, *Microsoft* ha segnalato alla Commissione europea che l'accuratezza del suo strumento di rilevazione dell'adescamento è dell'88%, il che significa che su 100 conversazioni segnalate è possibile che 12 siano escluse al momento della verifica, mentre l'accuratezza è più del 99% per l'identificazione di materiale pedopornografico, sia per quanto riguarda il materiale noto che quello nuovo. Vds. CE, *Impact Assessment Report*, *Annex* 8, *cit.*

sottoscritta nell'ambito del Consiglio d'Europa[9]. Essa ha come scopo principale la protezione dei minori contro lo sfruttamento e l'abuso sessuale, anche tramite l'introduzione di norme che puniscano tutte le forme di sfruttamento, sia *online* che *offline*. Prima della sua ratifica, il diritto penale italiano non conosceva una fattispecie destinata a reprimere gli atti di adescamento, e i giudici italiani potevano al più applicare, in forma tentata, il delitto di atti sessuali con minorenne di cui all'art. 609-*quater* del codice penale[10].

Il legislatore italiano ha, però, scelto di introdurre una fattispecie più ampia rispetto a quella prevista dalla Convenzione di Lanzarote. Quest'ultima, infatti, definisce l'adescamento di minori a fini sessuali come «la proposta di un incontro da parte di un adulto, mediante l'utilizzo delle tecnologie dell'informazione e della comunicazione, a un minore che non abbia raggiunto l'età minima stabilita [dalla legislazione nazionale], ai fini di commettere nei suoi confronti uno qualsiasi dei reati [di atti sessuali con minore o quelli relativi alla pornografia minorile], quando tale proposta sia seguita da atti concreti per ottenere tale incontro»[11]. La definizione italiana, invece, si discosta da quella fornita dalla Convenzione, ampliandola sotto quattro aspetti: 1) anticipando la soglia di punibilità a un momento precedente alla proposta di incontro e punendo qualsiasi atto volto a carpire la fiducia del minore; 2) estendendo la punibilità ai fatti commessi nei confronti di minori di età inferiore ai sedici anni, mentre l'età del consenso sessuale nell'ordinamento italiano è di quattordici anni; 3) attribuendo rilievo penale a qualsiasi forma di adescamento anche al di fuori del contesto di internet, 4) aggiungendo ulteriori reati-scopo oltre ai due reati specificati nelle normative europee[12].

L'estensione della punibilità ai fatti commessi nei confronti di minori di età inferiore ai sedici anni, quindi oltre l'età del consenso, può essere compresa alla luce dell'ampio raggio di delitti-scopo stabilito dal legislatore italiano. Infatti, mentre la Convenzione di Lanzarote e la direttiva europea specificano come delitti-scopo dell'adescamento solo i reati di atti sessuali con minorenne e di produzione di materiale pedopornografico, il codice penale italiano annovera anche molte altre fattispecie criminose a cui può essere mirato l'adescamento. Pertanto, qualora l'adescamento riguardi un minore di anni sedici che abbia compiuto i quattordici anni di età, la punibilità dipenderà dall'oggetto del dolo: se il delitto-scopo può essere posto in essere esclusivamente in danno di minori di anni quattordici, il delitto di adescamento non è configurabile[13]. Di conseguenza, adescare un quindicenne con l'intento di compiere atti sessuali consensuali con lui o lei, o di farlo o farla assistere al compimento di atti sessuali, non costituisce reato. Al contrario, il reato di adescamento è configurabile qualora il quindicenne venga approcciato con l'intento di produrre materiale pedopornografico, di favoreggiare la prostituzione minorile o di commettere violenza sessuale.

Merita attenzione anche il fatto che il nuovo reato di illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale (noti anche come "*deepfake*"), introdotto dal legislatore italiano con entrata in vigore il 10 ottobre 2025 come parte del recepimento dell'*AI Act* europeo, non è inserito tra i reati-scopo dell'adescamento[14]. La diffusione illecita di *deepfake*, infatti, di per sé non costituisce un reato sessuale, pertanto non è sufficiente che l'adescamento abbia come unico fine la creazione o l'alterazione di contenuti con un sistema di intelligenza artificiale. Se il *deepfake* ha un contenuto sessuale, però, lo scopo dell'adescamento non è il *deepfake* in sé, ma il reato sessuale che il *deepfake* realizza o agevola, tipicamente la produzione di materiale pedopornografico, reato più grave della diffusione illecita di *deepfake*. Inoltre, l'adescamento può avvenire anche con l'ausilio di contenuti *deepfake*, utilizzati per

---

9. *Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e gli abusi sessuali*, Lanzarote, 25 ottobre 2007 (https://rm.coe.int/16809f545d), ratificata dalla l. 1° ottobre 2012, n. 172 (vds., part., art. 4, lett. *z*).
Il reato di adescamento di minori è stato previsto anche dalla direttiva 2011/93/UE, del 13 dicembre 2011, che precede la modifica del codice penale, perciò l'art. 609-*undecies* cp può anche essere vista come attuazione implicita di una direttiva europea. L'attuazione della direttiva è avvenuta successivamente con il d.lgs 4 marzo 2014, n. 39, ma a quel punto il reato di adescamento dei minori era già stato introdotto nel codice penale. Vds. Ministero della giustizia, *Schema di D.Lgs. – Attuazione della direttiva 2011/93/UE in materia di lotta contro l'abuso e lo sfruttamento dei minori e la pornografia minorile – Relazione*, 21 novembre 2013 (www.giustizia.it/giustizia/it/mg_1_2_1.page? contentId=SAN966632#).

10. M. Vizzardi, *Sull'"adescamento" di minore tramite* social network *e il tentativo di atti sessuali con minorenne*, in *Diritto penale contemporaneo*, n. 1/2012, pp. 196 ss., part. p. 200.

11. Vds. art. 23 Convenzione di Lanzarote.

12. M. Vizzardi, *Il delitto di adescamento di minorenni (art. 609-*undecies*)*, in *Dir. pen. cont.*, 18 settembre 2015.

13. Cass. pen., sez. III, sent. 23 maggio 2018, n. 23173. Vds. anche S. de Bonis, *Capitolo X: Adescamento di minorenni*, in A. Cadoppi *et al.* (a cura di), *Diritto penale*, t. III, UTET Giuridica (WK), Milano, 2022, p. 6453.

14. Legge 23 settembre 2025, n. 132: «*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*».

manipolare o ingannare il minore. In tal caso, però, si configura esclusivamente il nuovo reato di illecita diffusione di *deepfake*, in quanto il reato di adescamento è configurabile solo se il fatto non costituisce più grave reato, e la diffusione illecita di *deepfake* è un reato più grave[15].

Tabella n. 1: La definizione di adescamento di minori nelle normative nazionali ed europee

	Convenzione di Lanzarote	**Direttiva 2011/93/UE**	**Codice penale italiano**
Anno di adozione	2007	2011	2012
Disposizione	art. 23	art. 6	art. 609-*undecies*
Condotta tipica	la proposta intenzionale di un incontro da parte di un adulto, *mediante l'utilizzo delle tecnologie dell'informazione e della comunicazione*, a un minore, quando tale proposta sia seguita da atti concreti per ottenere tale incontro	un adulto propone, *a mezzo di tecnologie dell'informazione e della comunicazione*, a un minore di incontrarlo, ove tale proposta sia stata seguita da atti materiali finalizzati a tale incontro	qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere *anche mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione*
Soggetto passivo	minore che non abbia raggiunto l'età minima stabilita	minore che non abbia raggiunto l'età del consenso sessuale	minore di anni sedici
Dolo specifico	ai fini di commettere uno qualsiasi dei seguenti reati: - atti sessuali con minore - produzione di materiale pedopornografico	intento di commettere i reati: - atti sessuali con minore - produzione di materiale pedopornografico	scopo di commettere i reati: - riduzione o mantenimento in schiavitù o in servitù - prostituzione minorile - pornografia minorile - detenzione di materiale pedopornografico - iniziative turistiche volte allo sfruttamento della prostituzione minorile - violenza sessuale - atti sessuali con minorenne - corruzione di minorenne - violenza sessuale di gruppo
Pena prevista	[non specificata, ma vds. art. 27]	pena detentiva massima di almeno un anno	reclusione da uno a tre anni

15. L'illecita diffusione di *deepfake* è punibile con la reclusione da uno a cinque anni, mentre per l'adescamento di minorenni è prevista la reclusione da uno a tre anni.

3. I limiti strutturali del rilevamento dell'adescamento nelle comunicazioni private

Oltre agli obblighi di rilevazione imposti ai prestatori di servizi di *hosting* e di comunicazione interpersonale[16], la proposta *Chat Control* prevede anche un obbligo di valutazione del rischio[17] che richiede necessariamente il monitoraggio su larga scala delle comunicazioni per identificare potenziali casi di adescamento.

Molto è stato detto e discusso riguardo alla possibile violazione dei diritti fondamentali di tale proposta[18]. Per permettere agli strumenti di monitoraggio automatici di identificare materiale pedopornografico, sia esso nuovo oppure noto, è necessario osservare il contenuto delle comunicazioni degli utenti prima che esso SIa criptato e spedito. Questo comporta, di fatto, una violazione del paradigma di crittografia *end-to-end*, che prevede la possibilità e salvaguarda il diritto di un utente di comunicare segretamente con una qualsivoglia controparte. Non intendiamo, però, dilungarci su questioni già ampiamente discusse in letteratura.

Non solo *Chat Control* propone un quadro legislativo per identificare sistematicamente materiale pedopornografico, ma mira anche a combattere il fenomeno dell'adescamento di minore, evidenziandone le lacune e le problematiche. In questo articolo ci concentriamo sul fenomeno dell'adescamento.

Nella letteratura scientifica di ambito psicologico e criminologico, l'adescamento è solitamente descritto come un processo che si articola in sei fasi che precedono l'abuso[19]:

1) scelta della vittima e contatto iniziale;
2) formazione dell'amicizia virtuale;
3) consolidamento del legame confidenziale;
4) valutazione del rischio di essere scoperti;
5) crescita del grado di intimità e di reciproca mutualità del rapporto;
6) sessualizzazione (introduzione della tematica sessuale ed eventuali pressioni finalizzate all'incontro).

L'adescamento è un reato che consiste in atti preparatori all'abuso e può avvenire in diverse forme, quali la produzione di contenuti pedopornografici, la costrizione a prestazioni sessuali o l'abuso fisico. Nel caso in cui l'abuso venga effettivamente commesso, si configura il reato più grave che "assorbe" l'adescamento[20].

Esistono differenze importanti tra la definizione di «adescamento» fornita dalla letteratura psicologica e quella contenuta nella direttiva 2011/93/UE, a cui fa esplicito riferimento l'art. 2(o) della proposta *Chat Control*. L'ultima delle sei fasi definite dalla letteratura psicologica non prevede necessariamente l'esistenza di una proposta di incontro tra l'adescatore e il minore. Secondo Broome e colleghi[21], la letteratura suddivide gli adescatori in due categorie: i "*fantasy-driven*", orientati a raggiungere il *climax* sessuale esclusivamente *online*, e i "*contact-driven*", motivati dall'organizzazione di veri e propri incontri. Sempre secondo gli Autori, è difficile classificare gli adescatori in modo inequivocabile in queste due categorie, poiché entrambi adottano strategie perlopiù simili. Tuttavia, la direttiva europea definisce esplicitamente l'adescamento come un processo finalizzato all'incontro e circoscrive la proposta di regolamento soltanto a una tipologia di adescamento: quella che culmina con il tentativo di organizzare un incontro. Altre condotte chiaramente dannose per la psiche dei minori, quali la condivisione di materiale pornografico che ritrae adulti, e incluse nell'ultima fase del *grooming* precedentemente descritta, ricadono in una zona legislativa grigia.

Tenuta in considerazione la necessità, prevista dalla direttiva europea, di un comprovato tentativo di incontro, l'adescamento risulta identificabile soltanto nella sua fase finale, nei casi in cui l'adescatore sia di tipo *contact-driven*, quindi orientato all'incontro. Per distinguere se una proposta di incontro faccia parte

16. Vds. art. 7 proposta di regolamento (n. 2).

17. Vds. art. 3 proposta di regolamento (n. 2).

18. Vds. EDPB-GEPD, *Parere congiunto n. 4/2022*, *cit.*, n. 6; European Digital Rights (EDRi), *Chat Control: What is actually going on?*, 24 settembre 2025 (https://edri.org/our-work/chat-control-what-is-actually-going-on/); European Parliamentary Research Service (EPRS), *Complementary Impact Assessment on the proposal for a Regulation laying down rules to prevent and combat child sexual abuse*, Parlamento europeo, aprile 2023 (www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf).

19. M. Vizzardi, *Il delitto*, *op. cit.*, p. 2. Nella letteratura psicologica internazionale vds., ad esempio, R. O'Connell, *A Typology of Cyber Sexploitation and Online Grooming Practices*, Cyberspace Research Unit, University of Central Lancashire, 2003 (http://image.guardian.co.uk/sys-files/Society/documents/2003/07/24/Netpaedoreport.pdf).

20. M. Vizzardi, *Il delitto*, *op. cit.*, p. 13.

21. L.J. Broome - C. Izura - N. Lorenzo-Dus, *A systematic review of fantasy driven vs. contact driven internet-initiated sexual offences: Discrete or overlapping typologies?*, in *Child Abuse & Neglect*, vol. 79, maggio 2018, pp. 434-444.

di uno schema di adescamento o costituisca una semplice proposta di incontro tra due amici *online*, è necessario ricostruire e analizzare l'intero storico delle comunicazioni tra i due utenti. In mancanza di tale contesto, anche un messaggio del tutto innocuo, come "Ci troviamo domani alle 15 per un gelato?", potrebbe essere erroneamente segnalato come un tentativo di adescamento.

La natura della proposta *Chat Control* è massiva e preventiva, in quanto non si limita agli utenti individuati come sospetti sulla base di indagini di polizia. Questa impostazione, per le ragioni tecniche di cui sopra, implica la raccolta e l'analisi di un volume estremamente ampio di informazioni, relative a un numero indeterminato di utenti. Nel caso del materiale pedopornografico, data la sua natura prevalentemente audiovisiva, i sostenitori della proposta possono sostenere che il monitoraggio si limiti a immagini e video, riducendo parzialmente l'invasività nei confronti della *privacy* degli utenti. Tale argomento non è, tuttavia, applicabile al reato di adescamento, che si fonda in larga misura sulle comunicazioni testuali tra l'adescatore e la vittima. Di conseguenza, il rilevamento dell'adescamento richiede l'analisi delle comunicazioni testuali di tutti gli utenti di un servizio di comunicazione interpersonale.

Infine, si riscontra una mancanza di allineamento anche tra gli strumenti di identificazione e la definizione legale di adescamento. Ad esempio, "*Project Artemis*", sviluppato da *Microsoft*, ha un'accuratezza di rilevazione dell'adescamento dell'88%. Le informazioni disponibili su *Project Artemis* rivelano che lo strumento cerca schemi ricorrenti di parole chiave e frasi associate all'adescamento, incluse interazioni sessuali e tecniche di manipolazione come l'estraniamento dalla famiglia e dagli amici. Secondo quanto riportato da testate giornalistiche quali *NBC News*[22], e non da documenti tecnici, il sistema analizza le conversazioni e assegna loro un punteggio che indica la probabilità di adescamento in corso. Se la probabilità supera una certa soglia, le informazioni vengono controllate da un operatore umano.

Nonostante *Project Artemis* sia uno degli strumenti più conosciuti e i risultati riportati siano promettenti, sono state divulgate poche informazioni al riguardo. Non è chiaro, ad esempio, su quali dati sia stato sviluppato questo sistema; pertanto, non è possibile conoscere con certezza quali tipologie di contenuto sia in grado di identificare. Ciò è necessario per evitare che i predatori possano aggirare i meccanismi di identificazione, una volta venuti a conoscenza di tali meccanismi[23]. Basandoci sulle informazioni disponibili, possiamo ipotizzare che *Project Artemis* sia in grado di identificare tutti quei contenuti e quei comportamenti che potenzialmente appartengono alla sfera dell'adescamento – seguendo quindi la definizione in letteratura psicologica –, ma che non sia stato programmato per identificare specificamente solo le istanze di adescamento definite dalla direttiva 2011/93/UE. Questa ipotesi è ulteriormente rafforzata dal fatto che l'azienda responsabile di *Project Artemis* (*Microsoft*) non è un'azienda europea, bensì statunitense. Non solo gli Stati Uniti non sono soggetti al diritto comunitario, ma il loro sistema penale è caratterizzato da una marcata frammentarietà, in quanto ciascuno Stato federato gode di un'ampia autonomia in materia penale. Mentre esiste il reato federale di «*online enticement of a minor*»[24], limitato ai casi di adescamento via *Internet* (un'infrastruttura di competenza federale), gli Stati federati criminalizzano l'adescamento in maniera eterogenea, con definizioni, età del consenso e pene molto diverse[25]. Pertanto, rimane incerta la possibilità di utilizzare nel contesto europeo questi strumenti sviluppati nel contesto americano.

È interessante notare come, similmente a quanto discusso nella sezione successiva, il funzionamento di questi strumenti sia più compatibile con la definizione di «*grooming*» fornita da alcuni ordinamenti nazionali (come quello italiano, precedentemente presentato) rispetto alle definizioni più restrittive fornite dalla direttiva 2011/93/UE e dalla Convenzione di Lanzarote, le quali richiedono il sussistere di un tentativo conclamato di organizzare un incontro con un minore.

---

22. O. Solon, *Microsoft launches tool to identify child sexual predators in online chat rooms*, *NBC News*, 9 gennaio 2020 (www.nbcnews.com/tech/tech-news/microsoft-launches-tool-identify-child-sexual-predators-online-chat-rooms-n1112881).

23. C. Jee, *Microsoft has created a tool to find pedophiles in online chats*, in *MIT Technology Review*, 10 gennaio 2020 (www.technologyreview.com/2020/01/10/130941/microsoft-has-created-a-tool-to-find-pedophiles-in-online-chats)

24. 18 US.C., § 2422(b), il quale recita: «*Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life*». Vds. anche il caso *Stati Uniti c. Dhingra*, 371 Fed.3d 557 (9th Cir. 2004).

25. Per esempio, mentre nello Stato di New York è necessaria la proposta di incontro, in Texas e in California è stata adottata una definizione più ampia: vds. *New York Penal Code*, § 120.70 (*Luring a child*); *Texas Penal Code*, § 33.021 (*Online solicitation of a minor*); *California Penal Code*, § 288.3.

Sussistono, altresì, dubbi riguardo alla verifica dell'età effettiva degli utenti. La pratica basilare di richiedere agli utenti di autocertificare la propria età è facilmente aggirabile, in quanto gli utenti possono dichiarare il falso senza dover presentare alcuna documentazione a supporto. Alcuni Paesi, tra cui Francia, Spagna, Germania[26] e Italia[27], hanno recentemente introdotto l'obbligo, per le piattaforme che distribuiscono contenuti pornografici, di appurare l'età reale degli utenti[28], prescrivendo soluzioni tecniche che in futuro potrebbero essere estese anche alle piattaforme *social* generaliste. Tali disposizioni sollevano – ancora una volta – delicate questioni riguardanti il diritto alla *privacy* degli utenti *online*.

Per tentare di porre rimedio al problema senza dover sottoporre gli utenti a tali verifiche, le piattaforme hanno sviluppato diversi approcci, senza però divulgarne gli aspetti tecnici, in linea con quanto sottolineato poc'anzi. Ad esempio, nell'agosto del 2025, *YouTube* ha iniziato ad utilizzare un sistema che, tramite "*machine learning*" e una varietà di segnali, inclusi i tipi di video cercati dagli utenti, le categorie di video visualizzati, e la longevità dell'*account*, permette di identificare minori di 18 anni[29]. Queste dichiarazioni sono notevolmente generiche e non istanziate tecnicamente. Ad oggi, non è stato divulgato al pubblico alcun dettaglio tecnico su quali segnali siano effettivamente utilizzati e su quale peso abbiano nella decisione finale, né tantomeno su come e quale modello si basi il sistema.

Concentrandoci solamente sugli aspetti tecnici e astraendo dal caso specifico di *YouTube*, secondo la e*Safety Commissioner* australiana[30], le piattaforme potrebbero utilizzare alcune delle seguenti analisi per stimare l'età degli utenti:

- verifica dell'eventuale interazione del titolare dell'*account* con contenuti rivolti a minori di 16 anni;
- analisi del livello linguistico e dello stile espressivo utilizzati dal titolare dell'*account* e dagli utenti con cui interagisce;
- analisi dei contenuti visivi, come la stima dell'età facciale effettuata su fotografie e video caricati sulla piattaforma;
- analisi audio, come la stima dell'età della voce del titolare dell'*account*;
- modelli di attività coerenti con gli orari scolastici;
- connessioni con altri utenti che appaiono avere meno di 16 anni;
- appartenenza a gruppi, *forum* o comunità rivolti ai giovani.

Tuttavia, tale lista è solo un ventaglio di ipotesi che non rappresenta con accuratezza tecnica la soluzione specifica adottata da ogni piattaforma. Questo impedisce ulteriormente di valutare l'effettiva portata di tali soluzioni, nonché il loro impatto sul diritto alla *privacy* degli utenti.

In conclusione, nonostante taluni promotori siano dell'avviso che la proposta avrebbe un impatto positivo significativo nel contrastare il fenomeno dell'adescamento, noi siamo dell'opinione che la proposta presenti vari problemi, sia dal punto di vista giuridico che dal punto di vista tecnico. Per poter identificare taluni casi di adescamento di minore, senza nemmeno includere condotte psicologicamente dannose, quale la sessualizzazione *online*, *Chat Control* necessita di un accesso illimitato alle conversazioni private dei cittadini europei.

4. Il problema del disallineamento tra *Chat Control* e le norme europee

Nella parte precedente abbiamo mostrato la discrepanza tra le condotte identificabili come rischio e quelle effettivamente punibili secondo le normative europee, nonché i problemi derivanti da tale discrepanza. Un'ulteriore osservazione che merita attenzione è che tale discrepanza si riduce considerevolmente con riferimento alle legislazioni nazionali, tra cui quella italiana, che abbassano la soglia di punibilità. Il monitoraggio imposto dalla proposta *Chat Control* sembra essere più compatibile con la definizione italiana di adescamento, in quanto la condotta punibile non richiede una proposta di incontro con il minore.

---

26. A. Desmarais, *The age verification era: Which EU countries are restricting access to adult sites?*, *Euronews*, 17 novembre 2025 (www.euronews.com/next/2025/11/17/the-age-verification-era-which-eu-countries-are-restricting-access-to-adult-sites).

27. Art. 13-*bis* dl 15 settembre 2023, n. 123: «*Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonchè per la sicurezza dei minori in ambito digitale*» (23G00135 – www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2023-09-15;123).

28. Dopo un procedimento istruttorio avviato nel gennaio 2024, nell'aprile 2025 l'Autorità per le garanzie nelle comunicazioni italiana ha dato attuazione all'art. 13-*bis* dl cit. con la delibera 96/25/CONS, che adotta le modalità tecniche e di processo per l'accertamento della maggiore età degli utenti (www.agcom.it/provvedimenti/delibera-96-25-cons).

29. J. Beser, *Extending our built-in protections to more teens on Youtube*, *YouTube Official Blog*, 29 luglio 2025 (https://blog.youtube/news-and-events/extending-our-built-in-protections-to-more-teens-on-youtube/).

30. e*Safety Commissioner*, *How will the social media age restrictions affect me?*, 10 dicembre 2025 (www.esafety.gov.au/young-people/social-media-age-restrictions).

Al contrario, la direttiva europea e la Convenzione di Lanzarote richiedono un tentativo tangibile di organizzare un incontro; pertanto, una buona parte delle condotte monitorate non sono considerate criminali.

Come si evince dalla tabella n. 1, l'adescamento di minori comprende gli stessi due reati-scopo sia nella Convenzione di Lanzarote che nella direttiva europea 2011/93/UE: atti sessuali con minore e produzione di materiale pedopornografico. Inoltre, entrambe le fonti specificano la proposta di incontro come condotta tipica. Ci si chiede, dunque, perché sia necessaria una proposta di incontro per l'adescamento finalizzato alla produzione di materiale pedopornografico, dal momento che tale materiale può essere prodotto anche senza un incontro con il minore. Nel 2015, infatti, il Comitato di Lanzarote[31], che riunisce tutti gli Stati che hanno ratificato la Convenzione, ha adottato un parere che affronta proprio questo interrogativo[32]. Il Comitato ha riconosciuto che la definizione di adescamento contenuta nella Convenzione potrebbe non rispondere alle sfide presenti e future, perché alcune forme di comportamento *online* che possono essere traumatiche per i minori non sono esplicitamente coperte[33]. Il testo della Convenzione non è stato modificato, ma il parere suggerisce agli Stati di estendere la criminalizzazione anche ai casi in cui l'abuso sessuale avviene esclusivamente *online*, senza alcun incontro fisico[34].

È interessante osservare che il legislatore italiano ha esteso la criminalizzazione ancor prima che il Comitato di Lanzarote esprimesse il proprio parere. Molti altri Paesi europei hanno scelto una soluzione diversa. Al contrario della normativa italiana, che amplia la definizione di adescamento di minori, la soluzione più comune è mantenere la definizione circoscritta prevista dalla Convenzione di Lanzarote e dalla direttiva europea e, allo stesso tempo, introdurre altri reati per criminalizzare le condotte finalizzate all'ottenimento di materiale pornografico dal minore. Ad esempio, il codice penale spagnolo recepisce fedelmente la definizione di «adescamento» prevista dalla Convenzione di Lanzarote, mentre introduce un'ulteriore fattispecie che punisce chiunque contatti un minore per indurlo, con l'inganno, a fornire materiale pornografico o a mostrare immagini pornografiche che ritraggono o raffigurano un minore[35]. L'ordinamento italiano sembra essere, perciò, uno dei pochi nel panorama europeo ad aver scelto di adottare una definizione più ampia, invece di creare fattispecie separate per le condotte non coperte dalla Convenzione di Lanzarote e dalla direttiva europea[36].

Sul piano giuridico, il problema principale riguarda la divergenza tra le condotte individuate come «a rischio» dalla proposta *Chat Control* e quelle penalmente rilevanti secondo la Convenzione di Lanzarote e la direttiva 2011/93/UE. Ne deriva un rischio di sovra-inclusione, da un lato (monitoraggio di comunicazioni che non integrano reati secondo le normative europee), e di sotto-inclusione, dall'altro (esclusione di condotte dannose, ma non tipizzate a livello europeo). Tale disallineamento è particolarmente evidente se si considerano gli ordinamenti nazionali che hanno ampliato la nozione di adescamento abbassando la soglia di punibilità, come quello italiano e quello inglese, o che hanno introdotto fattispecie autonome per le condotte *online* non coperte dalle normative europee, come quelli spagnolo e belga. Ne risulta una frammentazione normativa che compromette l'armonizzazione europea e pone problemi di certezza del diritto e di uguaglianza di trattamento.

5. Conclusione

La proposta *Chat Control* prevede l'uso di sistemi automatizzati di rilevazione in grado di individuare *pattern* di rischio nelle comunicazioni interpersonali digitali. Tuttavia, se tali sistemi sono calibrati sulla definizione ristretta di adescamento del minore contenuta nella Convenzione di Lanzarote e nella direttiva europea 2011/93/UE, si rischia di rilevare soltanto i casi relativi all'ultima fase dell'adescamento, quella in cui viene formulata una proposta di

31. Il Comitato di Lanzarote è stato istituito per verificare l'attuazione della Convenzione di Lanzarote da parte degli Stati che l'hanno ratificata (www.coe.int/en/web/children/lanzarote-committee).

32. Comitato di Lanzarote, *Opinion on Article 23 of the Lanzarote Convention and its explanatory note*, T-ES(2015)04_en *final*, 17 giugno 2015 www.coe.int/t/dg3/children/News/T-ES - 2015 - 04_enFinalOpinionArticle23.pdf).

33. Vds. part. parr. 11, 17 e 19 del parere.

34. Vds. par. 20 del parere.

35. Art. 183-*ter* del codice penale spagnolo (legge organica n. 10/1995). Una scelta simile è stata fatta dal legislatore belga nel 2014 (artt. 377-*quater* e 433-*bis* del codice penale).

36. Un altro ordinamento che ha adottato questa soluzione è quello inglese. L'art. 15A del *Sexual Offences Act* del 2003, in vigore dal 2015 soltanto in Inghilterra e in Galles (e non in tutto il Regno Unito), definisce il delitto di «Comunicazione sessuale con minore» («*Sexual communication with a child*») come un atto volto a ottenere gratificazione sessuale e non richiede la progettazione di un incontro con il minore.

incontro, riducendo considerevolmente il numero di rilevazioni ed escludendo numerosi casi comunque penalmente rilevanti negli ordinamenti nazionali che hanno adottato una definizione più ampia. Se, invece, i sistemi vengono calibrati su una nozione ampia di adescamento, non conforme alle normative europee, si rischia di produrre un modello in cui la sorveglianza tecnologica oltrepassa la tipizzazione penale e di creare un serio problema di *over-detection*, con un elevato numero di falsi positivi. Ciò comporterebbe un carico sproporzionato per le autorità competenti e un'ingerenza significativa nel diritto alla *privacy* degli utenti[37].

È quindi comprensibile che la proposta *Chat Control*, così come formulata, abbia ricevuto numerose critiche e che queste abbiano ritardato l'*iter* di approvazione. I problemi qui sollevati rendono evidente la necessità di una riflessione coordinata, che tenga conto sia della tecnologia sia dell'armonizzazione penale e dei diritti fondamentali.

37. Infatti, in una recente sentenza, la Corte di Strasburgo ha stabilito che una legge che impone la decrittazione delle comunicazioni crittografate *end-to-end* non può essere considerata necessaria in una società democratica e viola, pertanto, il principio di proporzionalità: vds. il caso *Podchasov c. Russia*, n. 33696/19, del 13 febbraio 2024.