[TRADUZIONE DI CORTESIA – VERSIONE ORIGINALE IN LINGUA INGLESE]

9 Ottobre 2023

Senato della Repubblica Italiana
Piazza Madama
00186 Roma
Italia

Alla cortese attenzione delle e degli Onorevoli membri della Commissione Affari Costituzionali e della Commissione Giustizia

OGGETTO: Atto Senato n. 878 - Progetto di legge per la conversione in legge del decreto-legge n. 123 del 15 settembre 2023 - Osservazioni di Aylo sulla protezione e la tutela dei minori

---

Onorevoli Senatrici e Senatori,

desideriamo esprimere in questa sede il nostro impegno relativamente alle tematiche della affidabilità e della sicurezza online nonché il nostro interesse per le disposizioni contenute nel decreto-legge n. 123 del 15 settembre 2023 ("**decreto-legge**") discusso da queste Commissioni riunite nell'ambito dell'iter di conversione in legge. Ci sentiamo molto vicini alle questioni oggetto del decreto-legge, come la lotta alla disaffezione giovanile e la tutela della sicurezza dei minori nell'ambiente digitale.

Per il tramite di queste brevi osservazioni, intendiamo rassicurarvi circa il fatto che, in qualità di gestori di una delle piattaforme di social media per soli adulti più conosciute al mondo, siamo pienamente impegnati nel garantire affidabilità e sicurezza a tutti i cittadini, compresi i minori, così a tutti i nostri utenti, i nostri partner, i nostri oltre 1.400 dipendenti e le loro famiglie.

1. COS'È AYLO

Prima di tutto vorremmo cogliere questa occasione per presentarci ed esporre le finalità da noi perseguite. Il nostro team comprende designer, ingegneri, analisti, sviluppatori, redattori, addetti al marketing e professionisti del settore legale e della compliance. Condividiamo la ricerca dell'eccellenza lavorando al fianco delle menti più brillanti nei nostri settori.

Aylo ha costruito un'azienda tecnologica di successo con l'aiuto dei suoi dipendenti altamente qualificati e di uno dei pubblici adulti più coinvolti e inclusivi online. Le nostre piattaforme consentono ad adulti consenzienti di esplorare contenuti che aderiscono ai nostri valori fondamentali: consenso, libertà di espressione sessuale, autenticità, originalità e diversità. In linea con i nostri valori e il nostro modello di business, come riflesso nei nostri termini e condizioni di utilizzo e nelle nostre politiche sui contenuti, adottiamo una politica di tolleranza zero nei confronti di qualsiasi tipo di contenuto illegale e in particolare nei confronti di qualsiasi materiale pedopornografico o non consensuale, che non trova spazio sulle nostre piattaforme. Come spiegheremo, Aylo migliora continuamente le sue misure volte alla affidabilità e alla sicurezza, adottate al fine di combattere la presenza di contenuti illegali su Internet. Il percorso significativo che abbiamo intrapreso da molti anni, e che continuiamo costantemente a percorrere, ha determinato un livello di affidabilità e sicurezza elevato, non solo nell'industria degli adulti, ma nell'intero settore tecnologico online. Ogni piattaforma online ha la responsabilità morale di unirsi a questa lotta, che richiede un'azione collettiva e una vigilanza costante.

2. I MODELLI DI BUSINESS

I modelli di business di Aylo sono tecnologicamente simili a quelli delle piattaforme online tradizionali. Le nostre attività principali sono costituite da siti di streaming video gratuiti e su abbonamento, sui quali vendiamo pubblicità e raccogliamo abbonamenti per l'iscrizione. Le principali unità di business di Aylo sono le seguenti: piattaforme di condivisione video (VSP), siti a pagamento, piattaforme di contenuti per modelli e modelle, piattaforme pubblicitarie e piattaforme di videogiochi.

2.1. Piattaforme di condivisione video (tra cui PornHub e Youporn)

La nostra piattaforma di streaming video principale è Pornhub.com. Lanciato nel 2007, Pornhub è un sito di hosting e streaming di contenuti per adulti, gratuito e supportato economicamente da pubblicità, che consente ai visitatori di visualizzare i contenuti caricati da modelli e modelle verificati/e e da società terze di intrattenimento per adulti.

Le piattaforme di condivisione video consentono la visione generale e gratuita di contenuti per adulti da parte degli utenti, registrati e non. Esse consentono inoltre il caricamento di contenuti per adulti da parte di modelli/e e partner di contenuti verificati tramite documenti d'identità. Tutti i contenuti sono moderati da una dozzina di strumenti automatici e sono sottoposti alla revisione e all'approvazione di un moderatore umano prima di essere pubblicati.

Altri esempi delle nostre piattaforme di condivisione video sono Youporn.com, Redutbe.com e Tube8.com.

2.2. Siti a pagamento (incluso Brazzers)

I siti a pagamento sono piattaforme ad abbonamento accessibili solo agli utenti registrati e paganti. Sui siti a pagamento non ci sono contenuti generati dagli utenti e tutti i contenuti sono di proprietà o concessi in licenza ad Aylo, senza alcuna interazione tra gli utenti. I contenuti sono prodotti professionalmente in conformità alle leggi vigenti, anche con riferimento ai rigorosi requisiti di registrazione dell'età e del consenso delle persone coinvolte. In questo modello di business, i nostri ricavi derivano dagli abbonamenti degli utenti.

Esempi dei nostri siti a pagamento sono Brazzers.com, Realitykings.com, Men.com, Twistys.com, Mofos.com, Transangels.com, HentaiPros.com.

2.3. Piattaforme di contenuti per modelli e modelle (incluso MyDirtyHobby)

Nel nostro portfolio abbiamo anche MyDirtyHobby, una piattaforma di social network online per adulti che consente a modelli e modelle di interagire con gli utenti. E' destinata ad una utenza europea, con la maggior parte degli utenti residenti in Germania. Il sito web (e i contenuti) sono accessibili solo agli utenti registrati. Analogamente alle piattaforme di condivisione video, i contenuti provengono da modelli e modelle che hanno superato un processo di verifica tramite documento d'identità e tali contenuti sono soggetti a moderazione prima della pubblicazione con strumenti automatici e moderatori umani. MyDirtyHobby include anche una piattaforma di live streaming per i modelli e le modelle verificati, con moderatori umani attivi 24/7 per tutti i live streaming. Le nostre fonti di guadagno per MyDirtyHobby sono i gettoni/crediti e gli abbonamenti. Gli utenti possono interagire con i modelle e le modelle sulla piattaforma.

2.4. Piattaforma di videogiochi (NUTAKU)

Questa piattaforma consente l'uso, l'acquisto o il download dei giochi Free-to-Play [gratuiti, ndr] o Premium [a pagamento, ndr] ivi contenuti. Gli utenti registrati possono vedere e giocare e non ci sono contenuti generati dagli utenti né c'è interazione tra gli utenti. I giochi sono sviluppati da sviluppatori terzi e vengono sottoposti a un'accurata revisione da parte dei

moderatori di Aylo prima di essere pubblicati sulla piattaforma. I nostri ricavi relativi a NUTAKU sono gli acquisti nel gioco tramite gettoni/crediti, giochi premium e abbonamenti.

2.5. Piattaforma pubblicitaria (TrafficJunky)

La nostra piattaforma pubblicitaria TrafficJunky non è altro che un network pubblicitario che gestisce gli annunci che appaiono sui siti web delle piattaforme di condivisione video. TrafficJunky utilizza una piattaforma pubblicitaria con strumenti self-service e crediti prepagati che consente di fornire spazi pubblicitari agli inserzionisti. Gli annunci intermediati da TrafficJunky sono sottoposti a una scansione da parte di strumenti automatici e a moderatori umani prima della pubblicazione, e sul suo sito non vi sono né contenuti generati dagli utenti né interazione tra gli utenti.

3. L'IMPEGNO DI AYLO PER LA SICUREZZA

Il team di Aylo e tutte le piattaforme di Aylo operano secondo principi di affidabilità e sicurezza, principi che sono al primo posto in tutto ciò che facciamo. Il nostro obiettivo è quello di raggiungere e stabilire i più alti livelli di affidabilità e sicurezza. Ciò si basa non solo sulle nostre politiche interne e sul nostro team di moderazione, ma anche sulla nostre diverse partnership esterne e sulla tecnologia impiegata a tal fine.

Come spiegheremo in dettaglio più avanti, Aylo ha una politica di tolleranza zero nei confronti dei contenuti non consensuali ("CNC" o "NCC", Non-Consensual Content) e del materiale pedopornografico (*child sexual abuse material*, c.d. "contenuti CSAM" o "CSAM"). Tali contenuti sono contrari ai nostri valori, alle aspettative dei nostri dipendenti, ai partner e alla nostra attività d'impresa. Solo guadagnando la fiducia e il rispetto dei nostri stakeholder e del pubblico possiamo infatti continuare a essere una delle società di intrattenimento per adulti più conosciute e popolate al mondo.

Abbiamo implementato alcune tra le misure di salvaguardia più sofisticate nella storia delle piattaforme di condivisione di contenuti generati dagli utenti per prevenire ed eliminare il materiale illegale dal nostro sito. Ciò include la verifica obbligatoria del soggetto che effettua il caricamento del contenuto, il divieto di scaricare contenuti gratuiti, l'ampliamento della forza lavoro e dei processi relativi alle attività di moderazione dei contenuti, la collaborazione con decine di organizzazioni no-profit in 35 paesi del mondo attraverso il nostro Trusted Flagger Program e il nostro modulo di richiesta di rimozione dei contenuti.

Miglioriamo costantemente le nostre politiche di affidabilità e sicurezza per identificare, segnalare, rimuovere, rivedere e denunciare i contenuti illeciti. Ci impegniamo a fare tutto il possibile per garantire un'esperienza online sicura ai nostri utenti, il che comporta uno sforzo a tutto tondo per innovare e cercare sempre di fare di più. Aylo modera in modo più incisivo, rapido ed efficace di molte altre piattaforme popolari, sia all'interno che all'esterno dello spazio per adulti.

4. LE ATTIVITA' DI CONTROLLO DEI CONTENUTI DI AYLO

Aylo ha messo in atto numerosi meccanismi e procedure di controllo dei contenuti, come indicato di seguito.

4.1. Contenuti generati dagli utenti

Nel dicembre del 2020, Aylo ha disabilitato l'accesso ai contenuti generati dagli utenti quando gli account non sono verificati, sia per gli utenti che usufruiscono delle piattaforme gratuitamente che per gli abbonati. Da allora possono caricare contenuti sui nostri servizi solo

le società di produzione e i modelli e le modelle che hanno presentato un documento d'identità in corso di validità e superato un cd. *liveness test* [ovvero un test che consente di verificare che il soggetto che presenta il documento sia effettivamente esistente, ndr]. Siamo stati una delle prime grandi piattaforme online - per adulti e mainstream - ad adottare questa politica. L'adozione volontaria della verifica personale dell'utente per tutti gli utenti attivi, cioè quelli che caricano contenuti, rappresenta un cambiamento fondamentale nel modo di operare delle piattaforme online. Speriamo e ci aspettiamo che l'intero settore segua il nostro esempio.

4.2.Termini vietati

Aylo impone delle restrizioni alle modalità di interazione dei visitatori sui nostri siti web. Per evitare che i visitatori cerchino contenuti che possano violare i nostri termini e condizioni di servizio, manteniamo un elenco di oltre 34.000 termini di ricerca vietati in diverse lingue. Oltre alla ricerca, i termini vietati non possono essere utilizzati in altri campi di testo resi disponibili agli utenti, come quelli per l'inserimento di titoli, descrizioni, tag e commenti.

4.3. Moderazione tecnologica

I nostri moderatori umani sono supportati da una serie di strumenti tecnici in espansione, tra cui:

- Tecnologia di hashing per individuare contenuti noti di CSAM e non consensuali, utilizzando liste di hash fornite da diverse organizzazioni come la Internet Watch Foundation e STOPNCII.org.

- Tre livelli di strumenti di intelligenza artificiale per individuare contenuti CSAM non già noti.

- Moderazione testuale contestuale che analizza i commenti alla ricerca di molteplici comportamenti scorretti.

- Strumenti di fingerprinting che assicurano che il materiale precedentemente moderato e rimosso non possa essere ricaricato. La nostra tecnologia brevettata utilizza un hashing percettivo proprietario per rilevare il caricamento ulteriore di materiale precedentemente eliminato, anche nel caso in cui questo materiale sia stato manipolato nel tentativo di eludere le nostre misure di moderazione.

In generale, i nostri strumenti includono i seguenti: CSAI Match di YouTube, Photo DNA di Microsoft, Safer di Thorn, Content Safety API di Google, la moderazione testuale di Spectrum Lab, Mediawise di Vobile e la tecnologia brevettata di Alyo Safeguard. Prendiamo provvedimenti immediati contro tutti gli elementi che vengono rilevati come CSAM o come non consensuali da uno qualsiasi dei nostri strumenti e agiamo nei confronti dei responsabili del caricamento. I nostri strumenti di intelligenza artificiale utilizzano l'apprendimento automatico per rilevare i contenuti che potrebbero includere persone di età inferiore ai 18 anni, in modo da avvertire i nostri moderatori e aiutarli a impedire in modo proattivo la pubblicazione del materiale sulle nostre piattaforme.

4.4. Strumenti di segnalazione

Nel 2020 abbiamo lanciato il nostro programma Trusted Flagger. Oggi questa iniziativa consente a oltre 55 organizzazioni no-profit specializzate nella prevenzione di contenuti CSAM e CNC di segnalarci i contenuti che ritengono possano i nostri termini e condizioni di utilizzo. Prendiamo immediatamente tutte le misure appropriate e necessarie, che includono in ogni caso la revisione umana, contro qualsiasi contenuto identificato da un Trusted Flagger. I nostri Trusted Flaggers hanno anche accesso diretto al team di moderazione di Aylo.

Gli utenti (visitatori della piattaforma) possono anche segnalare contenuti che violano i nostri termini e condizioni di utilizzo compilando il nostro modulo di richiesta di rimozione dei contenuti (Content Removal Request - CRR). Anche in questo caso, prendiamo tutte le misure

appropriate e necessarie contro il contenuto segnalato, che è soggetto a una revisione umana in tutti i casi. Gli utenti possono anche segnalarci materiale potenzialmente in violazione alle nostre condizioni di utilizzo e/o illegale utilizzando le nostre funzioni di segnalazione di contenuti, di utenti e di commenti potenzialmente lesivi. Tutte le segnalazioni vengono mantenute riservate e noi esaminiamo tutti i contenuti che ci vengono segnalati. Inoltre, qualsiasi richiesta da parte delle forze dell'ordine è gestita specificamente dal nostro team legale e abbiamo sviluppato un portale per le forze dell'ordine per semplificare questo processo.

4.5. Procedure di segnalazione di contenuti CSAM

Tutti i contenuti identificati da Aylo come potenziali CSAM sono soggetti alla nostra procedura di gestione e segnalazione dei contenuti CSAM.

Disattiveremo e banneremo immediatamente qualsiasi account utente che carica contenuti CSAM e segnaleremo l'utente e qualsiasi contenuto al National Centre for Missing and Exploited Children (NCMEC). Viene inoltre esaminata la cronologia delle interazioni dell'utente coinvolto nel caso specifico con le nostre piattaforme e qualsiasi altro contenuto caricato dall'utente.

Qualsiasi contenuto CSAM identificato in questo processo viene sottoposto a fingerprinting utilizzando gli strumenti di fingerprinting di Aylo per evitare che venga caricato sulle nostre piattaforme anche se è stato manipolato prima di essere ricaricato.

I nostri Transparency Report sono uno strumento fondamentale di comunicazione aperta a tutti e includono una ripartizione dettagliata delle statistiche sul materiale moderato e rimosso. Da quest'anno abbiamo iniziato a redigere rapporti semestrali (invece che annuali come fatto in precedenza) e tutti i rapporti sono disponibili nel Trust & Safety Centre di Pornhub.

4.6. Il nostro impegno contro i contenuti non consensuali

Pornhub è una piattaforma di hosting e condivisione di contenuti per adulti, destinata esclusivamente all'uso da parte di adulti consenzienti. Abbiamo una politica di tolleranza zero contro i contenuti non consensuali (“CNC” o “NNC”, cioè “Non-Consensual Content”). I contenuti non consensuali non comprendono solo le immagini intime non consensuali (“IINC” o “NCII”, cioè “Non-consensual Intimate Images”), comunemente chiamati contenuti di "revenge porn" o abuso di immagini), ma anche qualsiasi contenuto che implichi atti non consensuali, la registrazione di materiale sessuale senza il consenso della persona o delle persone presenti, o qualsiasi contenuto che utilizzi le sembianze di una persona senza il suo consenso, ad esempio i deepfake.

Siamo fermamente impegnati a proteggere la sicurezza dei nostri utenti e l'integrità della nostra piattaforma. Siamo al fianco di tutte le vittime di contenuti non consensuali.

5. LA NOSTRA PRIMA OSSERVAZIONE IN RELAZIONE AL DECRETO-LEGGE: IN GENERALE, LE MISURE DI FILTRAGGIO E LE APP DI CONTROLLO PARENTALE POSSONO RAPPRESENTARE STRUMENTI EFFICACI, MA DEVONO ESSERE DISCUSSI CON TUTTE LE PARTI INTERESSATE.

5.1. Supportiamo un accesso facile a, e a migliori condizioni di utilizzo per, i sistemi di controllo parentale, mentre siamo sfavorevoli all'introduzione di sistemi di *age gating*.

Non accettiamo e non tolleriamo in nessun caso la presenza di minori sui nostri siti.

Da anni sosteniamo pubblicamente processi e tecniche efficaci di verifica dell'età e abbiamo sempre dichiarato che la verifica dell'età deve essere uno strumento di tutela efficace dei bambini e di garanzia per la sicurezza e la privacy degli utenti.

La nostra esperienza nel rispettare i requisiti di verifica dell'età in altre giurisdizioni, come lo stato della Louisiana negli Stati Uniti, dimostra chiaramente che la verifica dell'età a livello di piattaforma non funziona per proteggere i bambini online. Inoltre, coloro che sono alla ricerca di contenuti per adulti e che comprensibilmente non desiderano condividere le proprie informazioni personali per la verifica dell'età, finiranno inevitabilmente su siti senza criteri che non applicano la sicurezza, la privacy, il consenso o la moderazione dei contenuti. I rischi per la privacy legati alla verifica dell'età sono stati evidenziati di recente anche dal governo australiano, che ha deciso di non procedere alla verifica obbligatoria dell'età in quanto tale tecnologia è ancora agli inizi. È importante notare che la verifica dell'età a livello di piattaforma non solo non impedisce ai minori di accedere a materiale per adulti online, ma comporta addirittura diverse conseguenze negative: richiedendo agli adulti di fornire ripetutamente documenti d'identità o altre informazioni di identificazione personale a potenzialmente centinaia o migliaia di siti web, espone gli adulti al rischio di furto d'identità, di violazione di dati personali e di estorsione.

Esistono già molti sistemi di controllo parentale, come il filtraggio di contenuti inappropriati, la regolazione dell'uso e il monitoraggio delle attività. Per garantire che i sistemi di controllo parentale che si basano sul filtraggio funzionino efficacemente, ai fornitori di contenuti sessualmente espliciti potrebbe essere richiesto di implementare modifiche tecniche ai loro siti web per supportare al meglio tali sistemi di controllo parentale. In particolare, i fornitori potrebbero dover implementare l'etichetta "Riservato agli adulti" (*Reserved to adults*, c.d. etichetta "RTA"). L'etichetta RTA consente di bloccare un sito web dall'accesso dei minori tramite un programma di filtraggio. L'inserimento di un codice nei meta tag dell'intestazione della pagina consente il filtraggio tramite browser web, ISP, firewall/proxy server, plugin, barre degli strumenti, software di filtraggio commerciali e sistemi operativi. Ad esempio, un programma di filtraggio esiste come funzionalità standard di Windows. I siti web con tale etichetta RTA non sono accessibili ai minori una volta attivato il filtro. L'RTA non può essere aggirata perché fa parte dell'URL del sito web. L'etichettatura aiuta a proteggere i bambini dalla visione di contenuti online non adatti alla loro età, a patto che i genitori si assicurino di attivare i controlli parentali previsti. Pur fornendo una data protezione ai bambini, questa non è la soluzione più efficace.

Se si desidera un controllo efficace, la soluzione migliore e più efficace per proteggere i bambini e gli adulti è quella di identificare gli utenti una sola volta e alla fonte: tramite il loro dispositivo o il loro account sul dispositivo, e consentire l'accesso a tutti i materiali e siti web vietati in base all'età a livello globale sulla base di tale identificazione. Ciò significa che gli utenti verrebbero verificati una sola volta, attraverso il loro sistema operativo, e non su ogni sito soggetto a restrizioni d'età. Questo riduce drasticamente i rischi per la privacy e crea un processo molto semplice da applicare per le autorità di regolamentazione e da seguire per gli utenti: oltre il 95% dei dispositivi in tutto il mondo è alimentato da sistemi operativi di proprietà di tre società.

Una volta che la verifica dell'età è effettuata la prima volta, sul dispositivo, dalle aziende che sviluppano i sistemi operativi e dai produttori di dispositivi, le quali già detengono i dati personali dei loro utenti, questi ultimi non sono incoraggiati a condividere più volte le loro informazioni di identificazione personale sui vari siti.

L'introduzione di una verifica dell'età a livello di dispositivo significa anche che i siti per adulti possono essere bloccati dai dispositivi dei minori per impostazione predefinita, che non è

necessario fare affidamento sulle piattaforme per conformarsi e che non c'è bisogno di un'applicazione individuale per le migliaia di singoli siti, rendendo così l'applicazione molto più efficace ed efficiente in termini di costi e risorse. Infine, non c'è nemmeno il rischio di deviare il traffico degli utenti, spingendo gli utenti che non vogliono rivelare le proprie informazioni personali per accedere a un sito web specifico dai siti che rispettano le leggi a quelli meno sicuri e non rispettosi delle leggi.

L'industria degli adulti, le ONG e le forze dell'ordine si sono dimostrate favorevoli a queste misure efficaci di verifica dell'età a livello di dispositivo e questa soluzione è adatta allo scopo a livello globale, garantendo un effetto immediato al momento dell'aggiornamento del software da parte dei sistemi operativi e dei produttori di dispositivi.

5.2. Sostenere i genitori con l’educazione digitale

Le misure tecniche da sole non sono quasi mai sufficienti a risolvere le questioni sociali. Una protezione adeguata ed efficace dei minori non potrà mai funzionare in modo significativo senza la partecipazione dei genitori. Affinché ciò avvenga, i genitori devono innanzitutto essere in grado di partecipare in modo significativo. Diversi studi dimostrano che i genitori non conoscono a sufficienza i modi per proteggere i diritti dei loro figli online. I genitori dovrebbero essere istruiti nel modo più completo possibile sul comportamento tipico dei bambini e degli adolescenti su Internet. In particolare, dovrebbero essere informati su come i loro figli utilizzano Internet e su quali sono i pericoli e le opportunità per i loro figli. I genitori potrebbero controllare meglio il comportamento online dei loro figli attraverso una migliore educazione digitale. Apprezziamo qualsiasi impegno nel decreto-legge volto a migliorare l'educazione dei genitori in questo senso.

5.3. Misure tecniche di controllo parentale

Nel contesto attuale, i genitori possono utilizzare meglio sistemi di controllo parentale altamente efficaci come i filtri con una maggiore consapevolezza. In questo modo, i minori possono essere protetti tramite la semplice progettazione di filtri, poiché questi partono dalla radice di Internet, a differenza dei sistemi di verifica dell'età. Con questa consapevolezza, i genitori possono configurare le impostazioni del router per filtrare determinati contenuti. Le impostazioni DNS del router in questione possono essere modificate in modo che il router si basi su un server DNS "salva minori". Inoltre, un tale DNS provvedere a bloccare i domini proxy e le VPN che eludono i filtri. Vengono bloccati anche i siti a contenuto misto (come Reddit e Imgur). Google, Bing, Yandex, DuckDuckGo e YouTube sono impostati in modalità sicura. Per software di filtro si intende un software installato sul dispositivo dell'utente finale per rilevare e filtrare i contenuti non adatti ai minori. La maggior parte di queste misure non richiede competenze tecniche avanzate, dispositivi di protezione speciali o software acquistati; possono essere impostate rapidamente e facilmente su (quasi) tutti i dispositivi. Il software di filtraggio verifica in background se il contenuto a cui si accede è appropriato per la fascia d'età. Di conseguenza, i siti web vengono visualizzati o bloccati dal software.

Di conseguenza, è chiaro che le misure di filtraggio e le app di controllo parentale possono essere efficaci, ma devono essere impostate in modo adeguato. Tuttavia, una buona normativa dovrebbe limitarsi a stabilire criteri generali e lasciare all'autorità competente, in questo caso per ora individuata nell'AGCOM, il compito di valutare, insieme a tutti gli stakeholder, comprese le piattaforme esperte nel settore, quali siano gli strumenti più appropriati, in un'ottica di bilanciamento tra esigenze di protezione dei minori ed esigenze di mercato e di libera espressione del pensiero e della sessualità.
Pertanto, il decreto-legge, come modificato e convertito in legge al termine del presente iter legislativo, non dovrebbe imporre criteri precisi e rigidi, in quanto questi potrebbero essere superati nel tempo.

6. LA NOSTRA SECONDA OSSERVAZIONE IN RELAZIONE AL DECRETO-LEGGE E AL DIBATTITO IN CORSO: L'AGE GATING NON È LA MISURA CORRETTA PER PERSEGUIRE LA TUTELA DEI MINORI.

Sappiamo che in Italia è in corso un dibattito sulla possibilità di introdurre l'obbligo di inserire un meccanismo di cd. *age gating* su alcune piattaforme online. Con le presenti osservazioni forniamo informazioni accurate che spiegano perché l'*age gating* non rappresenti la misura corretta per perseguire la tutela dei minori.

6.1. Il primo rischio: l'utilizzo di siti web non sicuri

I sistemi di verifica dell'età rigidi (anche detti sistemi di "*hard age gating*") si caratterizzano per il fatto di richiedere una sorta di certificazione dell'identità, rivelando così direttamente o indirettamente l'identità dell'utente alla piattaforma, o almeno a un sito di registrazione di una terza parte (legato all'utilizzo della piattaforma).

Nel caso in cui venisse implementato un sistema di verifica dell'età rigido su una specifica piattaforma per contenuti sessualmente espliciti, quasi nessun utente (a prescindere dall'età) continuerebbe a visitare tale sito. Gli utenti passerebbero semplicemente ad altri siti sprovvisti di sistemi di verifica dell'età e che, probabilmente, sarebbero meno ossequiosi della legge e soggetti a misure di affidabilità e sicurezza e di moderazione dei contenuti notevolmente inferiori. Data la disponibilità di un numero immenso di altri siti di questo tipo (privi di verifica dell'età/age gating), tale implementazione su un numero limitato di singoli siti avrebbe semplicemente gli effetti di una goccia nell'oceano. L'effettiva protezione dei minori sarebbe pertanto nulla, poiché gli utenti si sposterebbero semplicemente sui siti meno protetti e non ossequiosi della legge. Gli utenti che, per qualsiasi motivo, dovessero decidere di non spostarsi su altri siti, invece, utilizzerebbero altri metodi per aggirare i requisiti di protezione dell'età. Ciò può avvenire facilmente utilizzando le tecnologie VPN o Tor. Gli utenti più tecnologici, inoltre, potrebbero anche utilizzare altri strumenti di elusione, come strumenti di cd. *facial morphism* che consentono di rendere il proprio volto più anziano ai fini di un singolo utilizzo o di uno screening automatico dell'intelligenza artificiale. In un simile contesto, è anche da notare che chiunque, compresi i minori, sarebbe spinto a usare Tor per accedere al cosiddetto *dark web*. Una volta lì, è molto probabile che tali utenti sarebbero esposti a contenuti illeciti ed estremi con cui altrimenti non sarebbero mai entrati in contatto. Le conseguenze sociali negative nel caso di adozione di un simile strumento sarebbero dunque significative e del tutto inaccettabili. Esse sono del tutto evitabili attraverso l'implementazione di controlli a livello di dispositivo. Contenuti sessuali espliciti moderati e conformi alla legge possono peraltro aiutare gli adolescenti più grandi a soddisfare le loro esigenze di sviluppo e a esplorare la loro sessualità, in particolare nel caso della comunità LGBT+.

6.2. Il secondo rischio: i danni causati dai sistemi di verifica dell'identità e il legittimo interesse dei fornitori di piattaforme di condivisione video

Come dedotto in precedenza, l'implementazione di sistemi di verifica dell'età non ha alcun impatto positivo sugli interessi dei minori. Questo perché il livello e la quantità di consumo di contenuti sessualmente espliciti da parte dei minori non sono affatto influenzati da tali misure e, al contrario, i minori saranno incentivati a spostarsi verso siti dannosi e non conformi alla legge.

Peraltro, tali sistemi oltre a non tradursi in effetti positivi sulla protezione dei minori, finirebbero per ledere i legittimi interessi dei fornitori di piattaforme di condivisione di video, i quali verrebbero impattati negativamente in modo estremo. Qualsiasi richiesta di implementare un requisito di certificazione dell'identità sulle loro piattaforme porterebbe inevitabilmente a una perdita quasi totale di visitatori delle piattaforme stesse, che semplicemente passerebbero a

fare altro. Di conseguenza, l'esistenza stessa delle loro piattaforme verrebbe distrutta, poiché non avrebbero quasi alcuna possibilità di sopravvivere alla perdita totale di traffico sulle stesse.

Il risultato sarebbe assurdo e contrario ai diritti e alle libertà costituzionali fondamentali di tutte le parti interessate: i minori non sarebbero tutelati e, allo stesso tempo, i fornitori di piattaforme che applicano requisiti di accesso rigorosi sarebbero spazzati via dal mercato. Questo scenario equivarrebbe di fatto a un “esproprio” ingiustificato, in quanto i fornitori individuati verrebbero privati della loro esistenza commerciale senza alcun beneficio utile per i minori.

L'introduzione di sistemi di verifica dell'identità e dell'età finalizzati alla protezione dei minori dovrebbe essere determinata anche alla luce degli interessi degli utenti del sito web e dell'interesse pubblico generale. I sistemi di certificazione dell'identità e di verifica dell'età, e in particolare gli approcci basati sull'intelligenza artificiale come le tecnologie di riconoscimento facciale, potrebbero inoltre facilmente influire negativamente sui diritti e sui principi della protezione dei dati.

Ai sensi dell'art. 5, comma 1, lett. c del Regolamento generale sulla protezione dei dati (GDPR), i dati personali devono essere trattati in modo adeguato, pertinente e limitato a quanto necessario per le finalità per cui sono trattati. I sistemi di certificazione dell'identità utilizzati ai fini della verifica dell'età di una persona raccolgono per loro natura dati sensibili in maniera dettagliata. L'art. 9, comma 1 del GDPR considera tutti i dati personali relativi all'orientamento sessuale di una persona interessata come una categoria particolare di dati personali. Questi dati personali sono particolarmente sensibili. In quanto tali, essi godono di una tutela speciale ai sensi del GDPR. Il requisito secondo cui i dati devono essere limitati a quanto necessario deve dunque assumere un valore pregnante nel caso dei trattamenti concernenti dati personali sensibili.

Le tecnologie basate sull’intelligenza artificiale raccolgono i dati biometrici personali degli utenti (art. 9, comma 1 GDPR) e, in particolare, scattano e salvano immagini del volto dell'utente, creando un modello biometrico dello stesso.

Data l'assoluta mancanza di benefici comprovati in relazione all’utilizzo di rigidi sistemi di certificazione dell'identità / *age gating* a livello di sito web, non è né adeguato né pertinente né necessario ai sensi dell'art. 5 del GDPR ipotizzare di poter raccogliere e memorizzare i dati personali degli utenti ogni volta che un utente visiti un sito web di contenuti per adulti. Ciò è tanto più vero alla luce del fatto che i dati trattati nel caso specifico sono altamente sensibili, in quanto si riferiscono al consumo di contenuti sessualmente espliciti da parte di un individuo.

Inoltre, l'identificazione del visitatore può consentire la creazione di "profili utente" personalizzati che rintracciano, tracciano, analizzano e memorizzano le abitudini di consumo di contenuti sessualmente espliciti di ciascun utente. È difficile immaginare un dato personale più degno di essere protetto.

Gli utenti che utilizzano siti web con contenuti sessualmente espliciti sono fortemente interessati all'autodeterminazione in relazione ai propri dati. I dati raccolti sul loro comportamento d'uso riguardano la sfera più intima dei diritti della personalità, che comprende il loro orientamento sessuale e le loro preferenze sessuali. Se tali dati diventassero pubblici, ciò potrebbe avere conseguenze significative sulla loro vita familiare, sociale e professionale. I sistemi di certificazione dell'identità possono danneggiare in modo sostanziale il diritto all'autodeterminazione degli utenti dei siti web rispetto ai propri dati. I dati raccolti attraverso tali sistemi aumentano significativamente il rischio di hacking di tali dati. Inoltre, il rischio di

hacking dei sistemi di certificazione dell'identità riguarda in particolare gruppi vulnerabili come la comunità LGBT+.

In sintesi, i sistemi di certificazione dell'identità e di verifica dell'età a livello di sito web non rappresentano misure proporzionate alla luce della quantità di rischi che creano e dei danni che causano tanto agli utenti interessati quanto al sostentamento commerciale dei fornitori di piattaforme di condivisione video. Inoltre, verrebbero necessariamente applicati in modo arbitrario e diseguale, perché non potrebbero essere realisticamente applicati e imposti a tutti i siti web esistenti al mondo. Tali strumenti tendono a realizzare una “espropriazione” di fatto delle attività dei fornitori di tali piattaforme e violano i diritti fondamentali di cui alla Carta dei diritti fondamentali dell'UE. Allo stesso tempo, tali strumenti non sono utili nemmeno per il perseguimento degli interessi degli utenti stessi dei siti web, siano essi minori o adulti. Al contrario, tali strumenti arrecherebbero un danno significativo, violerebbero i principi di protezione dei dati e rappresenterebbero un rischio enorme per il diritto all'autodeterminazione degli utenti del sito web rispetto ai propri dati, creando inutili rischi di hacking per la grande quantità di dati personali altamente sensibili degli utenti che dovrebbero essere così raccolti.

7. TERZA OSSERVAZIONE IN RELAZIONE AL DECRETO LEGGE: IL SUO TESTO ATTUALE DEVE ESSERE RIVISTO IN MODO DA CHIARIRE IL RUOLO E LE DEFINIZIONI DEI SOGGETTI CHE OPERANO ONLINE

Infine, cogliamo l’occasione delle presenti osservazioni per sottolineare la necessità di chiarire alcuni aspetti specifici del decreto-legge, in particolare con riferimento al testo che ne individua il relativo campo di applicazione e le definizioni. Infatti, molti aspetti rimangono aperti, come le definizioni di "dispositivi" e "applicazioni", che sono così ampie da includere nella definizione di "dispositivi", ad esempio, qualsiasi dispositivo dell'"*Internet delle cose*". Inoltre, non esiste nel testo del decreto-legge una definizione di servizi di comunicazione elettronica e a questo proposito il coordinamento con altra normativa esistente potrebbe portare a conflitti nell'effettiva interpretazione del decreto-legge. Sotto tale aspetto, riteniamo che il testo debba essere rivisto per chiarire meglio il suo ambito di applicazione, il quale almeno nella *ratio* del decreto-legge, dovrebbe essere limitato alle sole aziende che forniscono servizi di telecomunicazione e ai produttori di dispositivi (quest’ultima, come detto, una definizione che si ritiene debba essere meglio definita).

8. CONCLUSIONI

Apprezziamo l’opportunità di poter discutere il sommo valore della protezione dei minori nel contesto online e dare evidenza dell'impegno costante di Aylo per la affidabilità e la sicurezza online, compreso il nostro lavoro per sconfiggere il fenomeno dei contenuti CSAM e non consensuali su tutte le nostre piattaforme e su Internet in generale. Siamo orgogliosi di essere leader in questo ambito, non solo tra le piattaforme di intrattenimento per adulti, ma anche tra i nostri pari nel panorama online. Il nostro impegno per la affidabilità e la sicurezza online è fondamentale per i nostri dipendenti, partner, membri della comunità e per il pubblico in generale, oltre che per il nostro obiettivo di diventare l'azienda di intrattenimento per adulti più affidabile e popolare al mondo.

Distinti saluti,

AYLO HOLDINGS S.À R.L.

[*sottoscrizione*]

Andreas Alkiviades Andreou

Manager Class A

[*sottoscrizione*]

Anis Baba

Manager Class A