ALL'ILL.MO GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

protocollo@pec.gpdp.it

Oggetto: Esposto formale per trattamento illecito di dati biometrici e violazione sistematica del GDPR da parte di OpenAI LP e soggetti terzi (Yoti Ltd, Stripe Identity).

Spett.le Garante per la Protezione dei Dati Personali,

Con la presente, il sottoscritto trasmette un esposto formale, corredato da dettagliato materiale probatorio, concernente il trattamento illecito di **dati biometrici sensibil**i e una **violazione sistematica e deliberata del Regolamento (UE) 2016/679** (GDPR) da parte di OpenAI LP, con il supporto dei servizi di Yoti Ltd e Stripe Identity.

Le condotte rilevate appaiono di rilevanza strategica, in quanto derivano da scelte architetturali e procedurali automatizzate, applicate su vasta scala a milioni di utenti per l'accesso a un servizio fondamentale come l'intelligenza artificiale generativa. Tali condotte, come illustrato nel presente esposto, non solo ledono i diritti fondamentali degli interessati, ma compromettono anche i principi cardine del GDPR quali la liceità, la proporzionalità e la trasparenza.

Tali pratiche sono espressione di un **disegno aziendale finalizzato a raccogliere un vasto database di dati biometrici** per ottenere un **vantaggio competitivo indebito**, tramite meccanismi ingannevoli ("**dark pattern**") che **coartano il consenso e sfruttano la posizione dominante**.

Le principali criticità evidenziate e approfondite nel presente esposto includono:

- Trattamento illecito di **dati biometrici sensibili**, in assenza di una base giuridica valida e di un consenso libero, specifico e informato.

- Pratica commerciale scorretta e ingannevole, che maschera la **raccolta obbligatoria di dati biometrici dietro un presunto obbligo normativo inesistente**.

- **Sproporzionalità** del trattamento rispetto alla finalità dichiarata, poiché la verifica biometrica non è né necessaria né l'unica via per tutelare i minori online.

- Violazione dei principi di "*Privacy by Design*" (Art. 25 GDPR) e di "minimizzazione" dei dati (Art. 5 GDPR), poiché il sistema è stato progettato per **massimizzare la raccolta di dati sensibili** anziché limitarla.

- **Rilevanza transfrontaliera** e possibile coordinamento internazionale, data la natura sistemica delle condotte e il coinvolgimento di soggetti operanti in diversi Paesi (USA e Regno Unito). Le architetture e procedure segnalate configurano violazioni di molteplici normative, tra cui il GDPR (in particolare Artt. 5, 7, 9, 12, 13 e 25), il Codice del Consumo (D. Lgs. 206/2005) e le Linee Guida europee sui "dark pattern".

Considerata la pervasività di tale strategia e il suo potenziale impatto sui diritti e sulle libertà fondamentali degli interessati, si chiede all'Autorità di avviare con urgenza un procedimento istruttorio. Tale azione risulta essenziale per accertare puntualmente le violazioni, porre fine immediatamente alle condotte che generano un vantaggio competitivo indebitamente acquisito tramite pratiche sleali e manipolazione dei diritti degli interessati, irrogare le sanzioni previste e adottare misure correttive atte a ripristinare il rispetto delle norme e a tutelare l'individuo e la sovranità digitale. Resto a completa disposizione per ogni eventuale chiarimento o integrazione che si rendesse necessaria.

Assunzione di Responsabilità e Consenso al Trattamento dei Dati Personali

Il sottoscritto,
Prof. Tommaso Gastaldi, afferente al Dipartimento di Statistica e il Dipartimento di Informatica, Laurea Magistrale in Cybersecurity, Sapienza Università di Roma (indirizzo email: tommaso.gastaldi@uniroma1.it),

presenta il presente esposto a titolo **esclusivamente personale**, precisando che l'istituzione di appartenenza è estranea ai contenuti e alle dichiarazioni ivi contenute.

Con il presente atto, il sottoscritto conferisce espressa autorizzazione all'Autorità Garante per la Protezione dei Dati Personali ("Garante Privacy") affinché possa trattare i dati personali forniti e il contenuto dell'esposto per le finalità connesse all'esercizio delle proprie funzioni istituzionali. Il consenso è rilasciato in maniera libera, informata, specifica e inequivocabile, sollevando il Garante Privacy da ogni ulteriore adempimento autorizzativo con riferimento alle finalità sopra indicate e nel rispetto della normativa vigente.

Con osservanza,

Documento trasmesso via PEC ai sensi dell'art. 65 del D.Lgs. 82/2005 (CAD)

Roma, 3 agosto 2025
Prof. Tommaso Gastaldi
Email: tommaso.gastaldi@gmail.com
Tel: +39 327 234 7610
PEC: tommaso.gastaldi@pec.it

ESPOSTO URGENTE ALL'ILL.MO
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Oggetto: Trattamento illecito di dati biometrici sensibili e consenso viziato per l'accesso a ChatGPT. Violazioni del GDPR da parte di OpenAI LP, Yoti Ltd e Stripe Identity.

Riepilogo

Il presente esposto denuncia il trattamento illecito di **dati biometrici sensibili** da parte di OpenAI LP, tramite Yoti Ltd e Stripe Identity, per l'accesso a ChatGPT, in violazione del Regolamento (UE) 2016/679 (GDPR) e del D.Lgs. 206/2005 (Codice del Consumo). Si contestano l'**assenza di una base giuridica valida**, il **consenso viziato tramite pratiche ingannevoli** ("**dark pattern**"), la **sproporzionalità** del trattamento e la mancanza di trasparenza, con gravi implicazioni per i diritti degli utenti e la sovranità digitale. Si richiede un'istruttoria urgente, sanzioni, la cessazione delle pratiche illecite ed anche la trasmissione all'AGCM per valutare profili anticoncorrenziali.

Soggetti chiamati in causa

Titolare del trattamento (presunto):

OpenAI LP, con rappresentante nell'UE OpenAI Ireland Ltd, 4 Earlsfort Terrace, Dublin 2, Irlanda.

Responsabili del trattamento (presunti):

Yoti Ltd, Company No. 08998951, Sede: 6th Floor, 107 Leadenhall Street, London EC3A 4AF, UK.

Stripe Identity (Stripe Inc.), 354 Oyster Point Boulevard, South San Francisco, California, 94080, USA.

Sommario dei fatti oggetto dell'esposto: OpenAI come "trojan" per la raccolta illecita di dati biometrici sensibili.

Il sottoscritto espone che, per accedere al servizio gratuito ChatGPT, l'utente è **obbligatoriamente sottoposto a una procedura di *"verifica dell'età"*** mediante la

raccolta di dati biometrici sensibili (*selfie* video o foto), delegata a Yoti Ltd, che analizza l'immagine per stimarne l'età cronologica. I punti salienti della procedura sono:

- presentata come requisito **obbligatorio** per l'utilizzo di ChatGPT (Allegato 1);

- **giustificata con il riferimento a un obbligo normativo europeo inesistente** nei termini dichiarati (Allegato 1);

- **irrinunciabile**, con esclusione dal servizio in caso di rifiuto (Allegati 2 e 3);
- causa di una **profilazione biometrica sproporzionata**, lesiva della **libertà digitale**, della **dignità dell'utente**, del **diritto all'accesso alla conoscenza** e dell'**inclusione digitale**.

---

1. **Violazioni riscontrabili**

1.1. Trattamento illecito di dati biometrici sensibili (Art. 9 GDPR, Art. 2-septies Codice Privacy, WP 29 Guidelines, CJUE, Causa C-311/18 – Schrems II)

La procedura di "verifica dell'età" tramite riconoscimento facciale messa in opera da OpenAI comporta il trattamento di **dati biometrici**. L'età stimata dal volto, così come i dati biometrici in sé, rientrano tra le "**categorie particolari di dati personali**" ai sensi dell'Art. 9 del GDPR, spesso definiti anche "**dati sensibili**". Tali dati possono essere trattati solo in presenza di un esplicito consenso, libero e non condizionato, o di una base giuridica esplicita (es. obbligo di legge o interesse pubblico rilevante)

Nel caso di specie:
– **non** esiste alcuna norma italiana (Legge n. 71/2017) o europea (DSA, Reg. UE 2022/2065) che imponga una **verifica biometricamente assistita per accedere a un'IA generalista**;
– il consenso è forzato: senza acconsentire al trattamento biometrico, l'utente è escluso dal servizio;
– la **Corte di Giustizia dell'Unione Europea (Causa C-311/18 – Schrems II)** ha stabilito che il **trattamento di dati biometrici**, essendo relativo a una categoria

speciale, è in linea di principio **vietato**, salvo che il titolare (OpenAI) dimostri l'adozione di misure rigorose, proporzionate e conformi – cosa che, nel caso in esame, non risulta effettuata.

Normativa citata da OpenAI/Yoti

OpenAI/Yoti fa riferimento, a giustificazione delle richieste, ad una normativa italiana (o europea) che imporrebbe di verificare l'età degli utenti per servizi digitali, con particolare attenzione ai minori. Spesso viene citata:
- La Legge italiana n. 71/2017 (che tutela i minori online),
- Il Regolamento UE 2022/2065 (Digital Services Act, DSA),
- Qualche riferimento generico al GDPR.

Sebbene vi siano ovviamente riferimenti a normative italiane o europee sulla protezione dei minori, nessuna di esse impone l'uso obbligatorio di tecnologie biometriche come quelle adottate da OpenAI/Yoti. Quindi, citare la legge italiana o europea come base per l'obbligo biometrico è un'interpretazione non corretta o comunque **fuorviante**. In pratica, OpenAI/Yoti si appoggiano a una norma reale (tutela dei minori), ma ne **travisano l'applicazione per imporre un trattamento dei dati più invasivo e non previsto**. Il riferimento è a una normativa reale, ma l'interpretazione o l'applicazione che ne fanno è sbagliata e **ingannevole**.

Cosa dice realmente la normativa

La Legge italiana n. 71/2017 tutela i minori da fenomeni di *cyberbullismo* e abuso, ma **non impone obblighi di verifica biometrica o raccolta dati per accedere a un servizio di intelligenza artificiale**.
– Il DSA introduce regole più rigorose per la protezione dei minori e il contrasto ai contenuti dannosi, ma non prescrive modalità biometriche obbligatorie per la verifica dell'età.
– Il GDPR impone condizioni stringenti per il trattamento di dati biometrici e richiede che il consenso sia libero, specifico, informato e inequivocabile.

Viene dunque usato un “**pretesto normativo**” che “non esiste nei termini indicati” — cioè non esiste la parte che giustifica la biometria obbligatoria.

1.2 Condivisione illecita di dati con terze parti (Artt. 26 e 28 GDPR)

La delega del processo di verifica a società terze (**Yoti** Ltd, **Stripe** Identity) solleva gravi dubbi sulla natura della relazione tra le parti. Come risulta dagli allegati (in particolare Allegato 2, che mostra un'email di OpenAI che **reindirizza l'utente a un link di Stripe** Identity), OpenAI utilizza più di un fornitore terzo. Si richiede al Garante di accertare se Yoti e Stripe operino come "Responsabili del trattamento" per conto di OpenAI o come "Titolari autonomi".
Nel primo caso, OpenAI violerebbe il GDPR per aver affidato un trattamento così invasivo a un soggetto terzo senza una base giuridica valida. Nel secondo, la pratica si aggraverebbe, configurando una condivisione illecita di dati personali e biometrici con terze parti per finalità commerciali non dichiarate, a danno dell'utente e in palese violazione del principio di limitazione della finalità (Art. 5.1.b GDPR).

Si richiede inoltre al Garante di **indagare su eventuali altri soggetti terzi coinvolti nella filiera di trattamento**, data sua evidente opacità, inclusi **provider infrastrutturali o subappaltatori non dichiarati**, al fine di mappare l’intera rete di responsabilità.

1.3 Consenso viziato e pratiche commerciali ingannevoli (Artt. 7 GDPR, 20 D. Lgs. 206/2005)

L’imposizione della verifica biometrica come unica condizione per accedere a ChatGPT configura un consenso viziato e una pratica commerciale ingannevole. Tale

prassi, qualificabile come “dark pattern” di tipo “forced action” (Linee guida EDPB WP259), manipola la volontà dell’utente, rendendo il consenso non libero, non informato e non revocabile senza conseguenze (Art. 7 GDPR). In particolare:

- Il consenso è **obbligato**, poiché il rifiuto comporta l’esclusione dal servizio, senza alternative meno invasive (es. autodichiarazione o verifica tramite SPID).

- È **non informato**, basato su una giustificazione normativa fuorviante che presenta la verifica biometrica come un obbligo legale, mentre nessuna norma europea, incluso il Regolamento UE 2022/2065 (DSA), la impone per servizi di IA generativa.

- È **non revocabile**, poiché l’utente non può sottrarsi al trattamento senza perdere l’accesso a ChatGPT.

Tale condotta configura altresì una **pratica commerciale scorretta** (Art. 20 D. Lgs. 206/2005), **inducendo l’utente in errore sulla presunta obbligatorietà del trattamento biometrico**, che è invece una scelta aziendale strategica volta a massimizzare la raccolta di dati sensibili.

1.4 Sproporzionalità del trattamento (Art. 5.1.c GDPR – Minimizzazione)

L’uso del riconoscimento facciale e del caricamento di documenti d’identità per la “verifica dell’età” è manifestamente **sproporzionato** rispetto alla finalità dichiarata (limitare l’accesso ai maggiorenni) e **non necessario**, violando il p**rincipio di minimizzazione** dei dati (Art. 5.1.c GDPR). Esistono alternative meno invasive, come l’autodichiarazione, la verifica tramite SPID o altri sistemi eIDAS, o l’uso di account già verificati, che OpenAI non ha considerato.
Inoltre, la **capacità di OpenAI di modulare e filtrare i contenuti** dell’IA in base al contesto e l’interlocutore rende la raccolta di dati biometrici ingiustificata e pretestuosa, configurando una scelta aziendale strategica non supportata da obblighi normativi.

Questo trattamento non solo è un **potenziale rischio discriminatorio per persone**

senza strumenti digitali idonei o con **caratteristiche fisiche non standard**, ma **la stessa biometria non identifica necessariamente la maturità del fruitore**.

L'assenza di metodi meno invasivi dimostra la **sproporzionalità** di tale trattamento. Alternative legittime e proporzionate, come l'autocertificazione con responsabilità legale, la verifica tramite SPID conformemente al Regolamento eIDAS (UE) 2014/910, o l'accettazione di un *disclaimer*, non sono state considerate. Ciò attesta che la scelta della biometria è una decisione strategica e deliberata di OpenAI, non giustificata da alcuna necessità normativa.

1.5 Assenza di trasparenza e informativa chiara (Art. 12–13 GDPR)

L'utente non riceve un'informativa completa su:
- chi conserva i dati biometrici (OpenAI, Yoti o entrambi?),
- per quanto tempo,
- se e come vengono anonimizzati,
- come può revocare il trattamento e ottenere la cancellazione.

1.6 Profilazione indiretta e finalità occulta

OpenAI, offrendo un servizio AI gratuito, veicola gli utenti verso Yoti, che può:

- **trattenere dati biometrici sensibili**,
- **monetizzare** i flussi di verifica,
- **profilare** utenti.

Questa canalizzazione di valore verso una terza parte commerciale, senza controprestazione per l'utente né trasparenza, configura una dinamica assimilabile a un meccanismo '**trojan-like**' per l'acquisizione di dati biometrici non giustificata da alcuna normativa esplicita.

Si offre un servizio utile (ChatGPT) e **generalista**, ma al contempo si **sottrae un dato sensibile per fini non dichiarati** e pretestusamente giustificati.

Questa prassi viola il **principio di limitazione della finalità** (Art. 5.1.b GDPR), poiché i dati personali, anziché essere trattati per la finalità dichiarata (accesso al servizio), vengono dirottati verso terze parti per **finalità commerciali di profilazione o monetizzazione** non esplicitamente comunicate all'utente.

1.7 Interesse collettivo violato: accesso libero all'IA e principio di legalità

L'intelligenza artificiale generativa è uno strumento pervasivo e generalista, essenziale per lo studio, la ricerca e l'inclusione digitale. Assimilare un tale servizio a una piattaforma destinata a **contenuti per adulti** è concettualmente **errato e pregiudica il bene comune**.

La richiesta di caricamento di dati biometrici o addirittura documenti di identità, spacciata per un **obbligo normativo inesistente**, non solo ostacola l'accesso a un bene di pubblica utilità e compromette il diritto all'informazione, ma si pone come un'**arbitraria imposizione di una prassi aziendale in totale spregio del principio di legalità**. In tal modo, un soggetto privato si arroga il potere di interpretare, e di fatto creare, un obbligo normativo che non trova riscontro nell'ordinamento giuridico nazionale ed europeo.

Tale condotta rappresenta **un grave affronto all'autorità del corpo giuridico della nazione e una pericolosa violazione dei diritti degli utenti**, i quali vengono **ingannevolmente indotti a credere che la limitazione del loro diritto all'accesso sia veramente basata su una legge**, quando in realtà è **solo una scelta strategica di OpenAI ed i suoi partner commerciali**.

1.8 Discriminazione algoritmica

L'uso di sistemi di stima dell'età basati sul riconoscimento facciale espone gli utenti a un potenziale trattamento **discriminatorio**. La letteratura scientifica evidenzia che tali **algoritmi possono presentare pregiudizi** ("*bias*") basati su caratteristiche etniche, di genere o fisiche, compromettendo l'accuratezza e rischiando di negare il servizio a determinati gruppi.
Tale prassi viola il principio di **equità e non discriminazione** del GDPR (Art. 5) e sarà ulteriormente regolata dall'*AI Act*, una volta pienamente operativo.

1.9 Violazione del principio di "Privacy by Design" (Art. 25 GDPR)

L'Art. 25 del Regolamento (UE) 2016/679 impone ai titolari del trattamento, come OpenAI LP, di implementare, fin dalla progettazione dei servizi, misure tecniche e organizzative appropriate per garantire che il trattamento dei dati personali rispetti i principi di **minimizzazione**, sicurezza e protezione dei diritti degli interessati. Tali misure devono includere, ad esempio, la **pseudonimizzazione** e la progettazione di sistemi che limitino la raccolta di dati sensibili, come quelli biometrici, solo quando strettamente necessario e proporzionato.

Nel caso di specie, OpenAI ha **deliberatamente progettato** il servizio ChatGPT in modo da imporre la **raccolta obbligatoria di dati biometrici** (*selfie* video o foto) tramite Yoti Ltd e altre società partner, configurando un "**data harvesting by design**" contrario a tale principio.

Questa scelta strutturale:
- **Non** adotta misure di **minimizzazione** dei dati, ma al contrario massimizza la raccolta senza giustificazione normativa,
- **Non** integra **salvaguardie** adeguate, come alternative meno invasive (es. **autodichiarazione o SPID**),

- Configura un sistema **intrinsecamente lesivo della privacy**, violando l'obbligo di proteggere i diritti degli utenti fin dalla fase di progettazione.

Tale condotta rappresenta **una chiara infrazione dell'Art. 25 GDPR**, **aggravata dalla mancanza di trasparenza e dal consenso viziato**, e richiede un intervento urgente del Garante per ristabilire la conformità normativa.

1.10 Violazione del Diritto Internazionale (Convenzione 108+)

La raccolta indebita di **dati biometrici e documenti d'identità** da parte di OpenAI contrasta con la **Convenzione 108+** per la protezione delle persone riguardo al trattamento automatizzato dei dati personali (Consiglio d'Europa, 1981, aggiornata 2018), ratificata dall'Italia. L'articolo 5 impone misure adeguate per proteggere i dati sensibili, e l'articolo 9 vieta trattamenti **sproporzionati** senza consenso libero. La pratica di OpenAI, imponendo la verifica biometrica come condizione per l'accesso a ChatGPT, viola tali principi, esponendo gli utenti a rischi transnazionali e **richiedendo un intervento del Garante in linea con gli standard europei e internazionali**.

1.11 Danno economico diretto

La procedura di verifica, che **richiede tempo e attrezzature specifiche**, comporta un costo significativo per gli utenti. Secondo stime basate su dati Statista 2025, con **circa 1 miliardo di utenti** ChatGPT e un tempo medio di 10 minuti per la verifica, si può ipotizzare un impatto economico collettivo rilevante. Tale prassi, aggravando il **danno per gli utenti**, configura una **pratica commerciale scorretta** ai sensi dell'Art. 20 D. Lgs. 206/2005.

1.12 Impatto Socioeconomico e Criminale della Raccolta Indebita di Dati Biometrici e Documenti

La pratica di OpenAI di **raccogliere indebitamente dati biometrici** (*selfie* video/foto) e **richiedere documenti d'identità** e persino **dati della carta di credito** tramite Yoti Ltd non solo viola il GDPR, ma alimenta un mercato globale illecito di dati personali, con gravi implicazioni socioeconomiche e di sicurezza pubblica. Dati statistici verificabili evidenziano la gravità di tale condotta:

Valore di mercato
Secondo il *Cost of a Data Breach Report 2024* di IBM, il costo medio di una violazione di dati biometrici è di 4,88 milioni di dollari, con un aumento del 10% rispetto al 2023. Sul **dark web**, i dati biometrici (es. scansioni facciali) sono venduti a prezzi che variano da 20 a 300 dollari per record, mentre **documenti d'identità completi (passaporti, carte d'identità)** possono raggiungere i 1.000-2.000 dollari, come riportato da *Forter* (2023) e *Cybersecurity Ventures* (2024).

Uso illecito
Il *UNODC Global Report on Cybercrime 2025* stima che il mercato nero dei dati personali generi annualmente oltre 1,5 trilioni di dollari, con i **dati biometrici utilizzati per frodi finanziarie, furti d'identità** e **accesso non autorizzato a sistemi sensibili**. Ad esempio, tutorial per falsificare impronte digitali sono venduti a 3 dollari su forum del **dark web**, secondo *Forter (2023)*.

Connessioni con la criminalità organizzata
Il *Federal Trade Commission (2025)* avverte che grandi database di dati biometrici sono obiettivi primari per gruppi criminali organizzati, che li sfruttano per riciclaggio di denaro e traffico illecito, come dimostrato da casi di hacking al porto di Anversa (*UNODC, 2023*).

Rischio concreto per gli utenti
Con oltre **1 miliardo di account ChatGPT attivi globalmente** (stima OpenAI 2024), la potenziale esposizione di dati sensibili a tali mercati rappresenta una minaccia

sistemica, aggravata dall'**assenza di trasparenza su conservazione e anonimizzazione** da parte di OpenAI.

Questa pratica non solo espone gli utenti a rischi concreti di abuso, ma contribuisce indirettamente a un'economia criminale che mina la sicurezza nazionale e internazionale. Si richiede al Garante di considerare tali evidenze come **aggravante**, imponendo **misure immediate per la cessazione della raccolta** e la **sanitizzazione** (o ***wiping***) totale e **digitalmente irrecuperabile dei dati già acquisiti**, al fine di **proteggere l'interesse pubblico e prevenire ulteriori danni**.

1.13 Violazione della Mission Dichiarata

OpenAI LP, nel suo *Charter* ufficiale (disponibile su openai.com/charter), dichiara come missione primaria "*assicurare che l'intelligenza artificiale generale (AGI) benefici tutta l'umanità*" e stabilisce un "*dovere fiduciario primario verso l'umanità*", impegnandosi a costruire AGI sicura e benefica e a minimizzare i conflitti d'interesse.

"OpenAI's mission is to ensure that artificial general intelligence (AGI)—by which we mean highly autonomous systems that outperform humans at most economically valuable work—benefits all of humanity. […]
***Our primary fiduciary duty is to humanity**."*

Tuttavia, la pratica di raccolta obbligatoria di dati biometrici tramite Yoti Ltd per l'accesso a ChatGPT **contraddice tali principi** almeno nei seguenti aspetti.

- Contraddizione con la mission: L'imposizione di un "**data harvesting by design**" e la profilazione indiretta degli utenti, senza base normativa valida, compromettono il beneficio collettivo e l'accesso inclusivo all'IA, violando il diritto all'informazione e alla conoscenza (Artt. 21 e 41 Costituzione Italiana).

- Danno agli investitori: Tale condotta, in contrasto con la mission dichiarata, mina la **fiducia degli investitori** (es. Microsoft, Nvidia, SoftBank), che hanno finanziato

OpenAI (valutazione $157 miliardi nel 2024) sulla base di un **impegno etico**, configurando un **potenziale inadempimento contrattuale e un danno reputazionale**, rilevante anche ai fini del Codice del Consumo (Art. 20 D. Lgs. 206/2005).

- **Principio di buona fede**: La divergenza tra mission dichiarata e **pratiche operative viola il principio di correttezza e buona fede** (Art. 1175 Codice Civile), inducendo gli utenti e gli *stakeholder* in errore sulla natura del servizio offerto.
Si richiede al Garante di valutare tale incoerenza come **aggravante**, dato l'impatto pubblico e la diffusione online di questo esposto, che evidenzia un tradimento sistematico degli impegni assunti da OpenAI.

1.14 Impatto sulla Concorrenza e sui Consumatori: Interesse dell'AGCM

La pratica di OpenAI di imporre la **raccolta obbligatoria di dati biometrici** (nonché di **documenti d'identità** e persino di **dati di carte di credito**) per accedere a ChatGPT non solo **viola il GDPR**, ma c**onfigura una condotta potenzialmente anticoncorrenziale e lesiva dei consumatori**, giustificando anche l'intervento dell'Autorità Garante della Concorrenza e del Mercato (AGCM). I seguenti elementi supportano tale tesi:

- Vantaggio competitivo sleale: Imponendo un "**data harvesting by design**" come condizione d'accesso, OpenAI accumula un database di dati biometrici e personali di oltre 1 miliardo di utenti (stima OpenAI 2024), un asset strategico che può essere sfruttato per migliorare i propri modelli di IA o condividerlo con Yoti Ltd, distorcendo la concorrenza nel mercato dell'intelligenza artificiale generativa. Ciò crea una barriera all'ingresso per competitor più piccoli (es. startup europee), che non dispongono di risorse simili, in violazione dell'articolo 2 della Legge 287/1990 (norme antitrust italiane) e dell'articolo 102 del Trattato sul Funzionamento dell'UE (abuso di posizione dominante).

- Pratiche commerciali scorrette: La presentazione della verifica biometrica come obbligo normativo inesistente (Allegati 1-3) costituisce un "dark pattern" di tipo "forced action", manipolando i consumatori e violando l'articolo 20 del Codice del Consumo (D. Lgs. 206/2005). Tale pratica inganna gli utenti, inducendoli ad accettare un trattamento invasivo per paura di perdere l'accesso a un servizio essenziale, con un impatto diretto sulla loro autonomia decisionale.

- Danno alla concorrenza e ai consumatori: L'**accumulo di dati sensibili** permette a OpenAI di profilare indirettamente gli utenti e potenzialmente **monetizzarli**, creando un modello di **business asimmetrico** che penalizza *competitor* etici e consumatori ignari. Secondo il *European Data Market Study 2024*, **il mercato dei dati personali in Europa vale 80 miliardi di euro**, e pratiche come questa amplificano la concentrazione di potere nelle mani di pochi giganti tech, compromettendo la pluralità e l'innovazione.

Si richiede pertanto al Garante Privacy anche di **trasmettere copia di questo esposto all'AGCM per un'indagine anche sugli aspetti di sua pertinenza**, al fine di valutare sia le violazioni privacy sia le implicazioni **anticoncorrenziali e commerciali**, garantendo una tutela olistica degli interessi pubblici italiani ed europei.

2. Riferimenti normativi e fonti

Regolamento (UE) 2016/679 – GDPR, Artt. 5 (principi applicabili al trattamento), 7 (condizioni per il consenso), 9 (categorie particolari di dati), 12-13 (trasparenza), 22 (decisioni automatizzate), 83 (sanzioni).

Regolamento (UE) 2022/2065 – DSA, Artt. 28 (trasparenza dei sistemi), 34 (valutazioni dei rischi sistemici).

Codice in materia di protezione dei dati personali (D.Lgs. 196/2003 e successive modifiche), art. 2-septies (dati genetici, biometrici e sanitari).

Codice del Consumo (D. Lgs. 206/2005), Artt. 20, 21, 22 (pratiche commerciali scorrette).

Linee guida EDPB WP259 sul consenso (2018).

Provvedimento del Garante n. 9751323/2022 – Sanzione a Clearview AI per trattamento illecito di dati biometrici.

Fonti varie: RaiNews, Privacy Network, garanteprivacy.it, Wired.it, Reddit, Euractiv.

---

3. Precedenti significativi

Caso Clearview AI

Il Garante italiano ha comminato una sanzione di €20 milioni a Clearview AI per trattamento illecito di dati biometrici.

Rilevate gravi violazioni: assenza di base giuridica, mancanza di consenso valido, violazione dei principi di minimizzazione, trasparenza e finalità.

Ordinata la cancellazione dei dati e il divieto di ulteriori trattamenti biometrici in Italia.

Ulteriori sanzioni europee

Olanda: €30,5 milioni di multa nel 2024 per trattamento illecito di dati biometrici, anche se pubblicamente disponibili online.

Francia: divieto d'uso del servizio per violazioni analoghe del GDPR.

Paralleli con il caso OpenAI / Yoti / Stripe Identity

Come nel caso Clearview AI:

- Si effettua un trattamento di dati biometrici (*selfie* e documenti).
- I dati sono raccolti da soggetti terzi (Yoti Ltd, Stripe Identity).
- Il consenso è condizionato all'uso del servizio, integrando possibili dark patterns.
- Viene evocata una base normativa inesistente o ingannevole, disorientando il consumatore.

La pratica configura, nei fatti, un trattamento illecito e sproporzionato, privo di una base giuridica solida e non conforme ai principi di necessità e proporzionalità.

---

4. Richieste al Garante Privacy

Alla luce dei fatti sopra esposti, chiedo formalmente che l'Autorità:

- Apra un'istruttoria sul trattamento dei dati biometrici da parte di OpenAI e dei fornitori terzi (Yoti Ltd, Stripe Identity).

- Verifichi la validità del consenso, accertando se la modalità adottata costituisca un dark pattern (es. forced action), in violazione delle Linee guida EDPB WP259.

- Accerti la mancanza di una base normativa valida, l'eventuale inganno o forzatura nei confronti dell'utente, e la sproporzione del trattamento rispetto alla finalità dichiarata.

- Indaghi sulla natura della relazione contrattuale tra OpenAI e i soggetti terzi (Yoti e **Stripe Identity**), per stabilire:

- Se esiste una **contitolarità** o una **comunicazione illecita** di dati.

- Se è stato effettuato un Transfer Impact Assessment (TIA), dato il possibile trasferimento di dati verso Paesi extra-UE.

- Ordini la **cessazione immediata** delle pratiche di **raccolta biometrica sproporzionata**, con adeguamento entro 30 giorni.

- Applichi le **sanzioni amministrative massime** previste dall'art. 83 GDPR, proporzionalmente alla gravità e al carattere transnazionale del trattamento (fino al 4% del fatturato annuo globale), tenendo anche conto delle **aggravanti evidenziate** nel presente esposto.

- Disponga la **cancellazione immediata e non tecnologicamente recuperabile (data wiping) dei dati** biometrici, dei documenti di identità e dei dati delle carte di credito degli utenti italiani già raccolti, nel rispetto del principio di minimizzazione (art. 5.1.c GDPR) e in coerenza con il provvedimento sanzionatorio a Clearview AI (n. 9751323/2022).

Tutela della sovranità digitale nazionale

Si chiede inoltre che l'Autorità valuti la **compromissione della sovranità digitale italiana**, segnalando che la raccolta e conservazione di dati sensibili da parte di un soggetto extra-UE (OpenAI LP, USA), in assenza di garanzie adeguate, rappresenta

un **rischio sistemico per la sicurezza e l'autodeterminazione dei cittadini italiani**, **in possibile violazione anche dell'art. 16 della Costituzione Italiana** (libertà personale).

Trasmissione all'AGCM e possibile coordinamento con istituzioni europee ed estere per appurare la filiera di trattamento dati e l'impatto sul mercato

Si richiede che il presente esposto sia trasmesso all'Autorità Garante della Concorrenza e del Mercato (AGCM) per l'apertura di un procedimento parallelo, data l'evidente **connessione tra le violazioni privacy** e le possibili **pratiche commerciali scorrette e anticoncorrenziali da parte di OpenAI**, ai sensi del D. Lgs. 206/2005 (Codice del Consumo) e della Legge 287/1990 (Tutela della concorrenza).

Si invita altresì rispettosamente il Garante a considerare la possibilità di un coordinamento con l'*European Data Protection Board* (EDPB) per garantire un approccio coerente a livello europeo. Si suggerisce inoltre di avviare, ove applicabile, un dialogo con la **Federal Trade Commission (FTC)** per il versante statunitense, data la natura transfrontaliera del trattamento e il coinvolgimento di soggetti operanti nel Regno Unito (Yoti Ltd) e negli Stati Uniti (Stripe Identity/OpenAI LP). Tale coordinamento è volto a valutare l'intera **filiera transnazionale di trattamento illecito**, incluse le implicazioni globali sul mercato, in linea con il meccanismo di cooperazione previsto dal GDPR (Artt. 60-76).

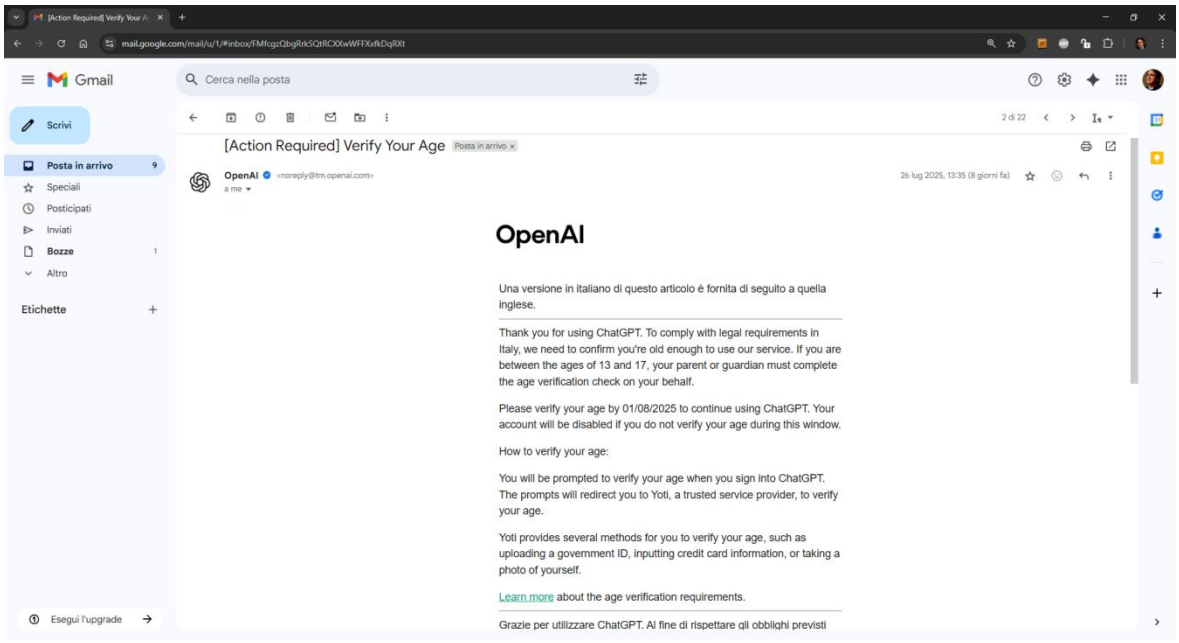
Si sollecita inoltre il Garante a segnalare all'FTC eventuali violazioni transfrontaliere che possano configurare pratiche commerciali sleali o **ingannevoli** (*deceptive*) ai sensi del ***Federal Trade Commission Act*** (15 U.S.C. §§ 41-58), con particolare riferimento alla raccolta indebita di dati biometrici. Tale segnalazione potrebbe supportare un'indagine analoga anche negli Stati Uniti, contribuendo a tutelare i consumatori e a mappare l'impatto economico di tali pratiche in un mercato globalizzato.

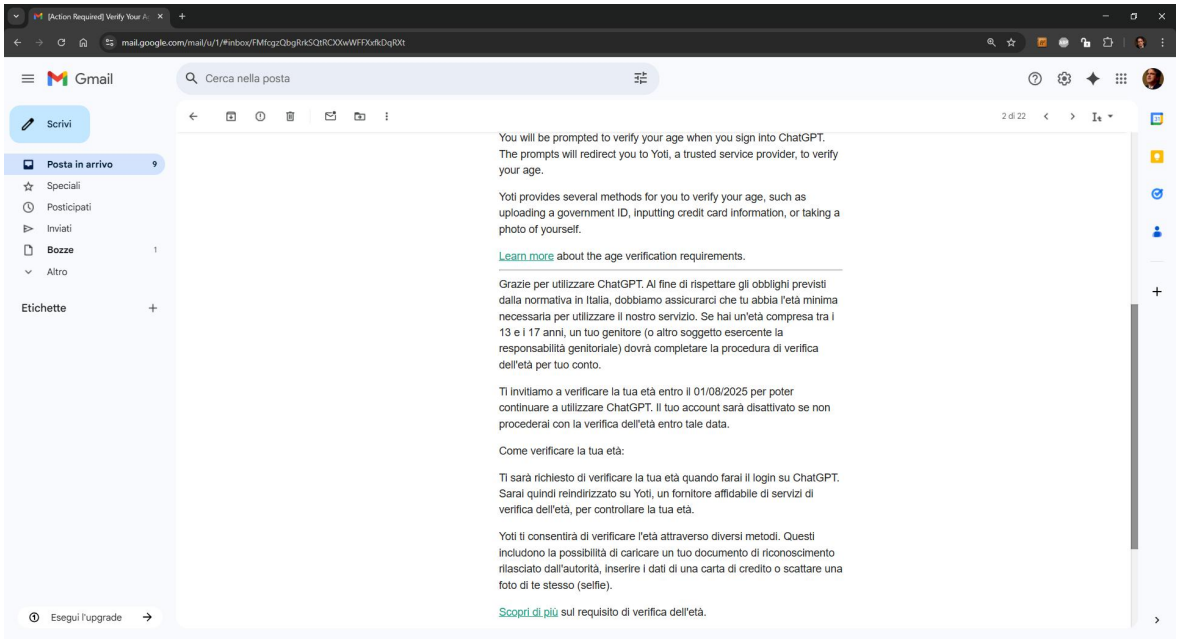
Allegati a supporto dell'esposto

Seguono allegati come prova, sebbene la prassi sia ormai nota agli utenti e non necessiterebbe di essere ulteriormente documentata.
La sequenza di schermate dimostra l'evoluzione **da una richiesta generica di età a una raccolta invasiva di dati biometrici**.
Le opzioni offerte impongono **entrambe l'uso della telecamera per la ripresa di un *selfie***, in palese contrasto con il **principio di minimizzazione** dei dati.

Tale prassi, che arriva ad includere l'*upload* di un **documento d'identità** o dei **dati della carta di credito**, nel contesto dei metodi proposti per la "verifica dell'età", sconfina nell'inaccettabile e costituisce un'ulteriore conferma della **sproporzionata** e **illegittima** raccolta dati da parte del Titolare.

- Allegati -





Allegato 1: Screenshots. Schermata richiesta età obbligatoria, pena disattivazione (data: Jul 26, 2025, 1:35 PM).

- Testo in Allegato 1 da OpenAI <noreply@tm.openai.com>, Jul 26, 2025, 1:35 PM: (Verificare l'eta o account disabilitato)

"Grazie per utilizzare ChatGPT. Al fine di rispettare gli obblighi previsti dalla normativa in Italia, dobbiamo assicurarci che tu abbia l'età minima necessaria per utilizzare il nostro servizio. Se hai un'età compresa tra i 13 e i 17 anni, un tuo genitore (o altro soggetto esercente la responsabilità genitoriale) dovrà completare la procedura di verifica dell'età per tuo conto.
Ti invitiamo a verificare la tua età entro il 01/08/2025 per poter continuare a utilizzare ChatGPT. Il tuo account sarà disattivato se non procederai con la verifica dell'età entro tale data.
Come verificare la tua età:
Ti sarà richiesto di verificare la tua età quando farai il login su ChatGPT. Sarai quindi reindirizzato su Yoti, un fornitore affidabile di servizi di verifica dell'età, per controllare la tua età.

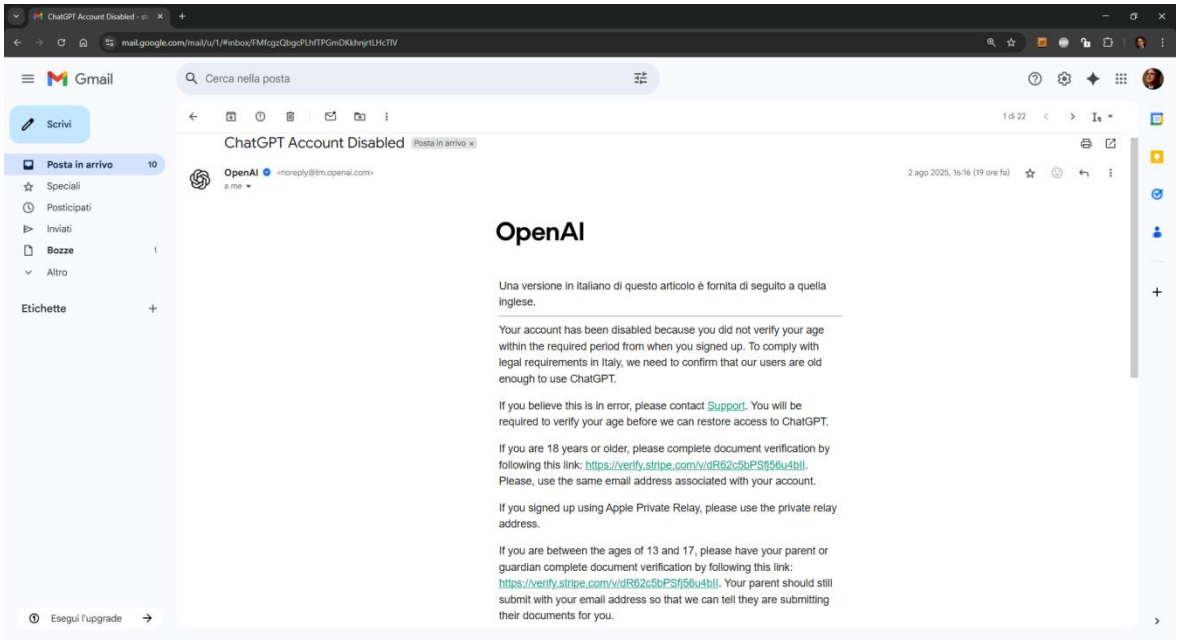
Yoti ti consentirà di verificare l'età attraverso diversi metodi. Questi includono la possibilità di **caricare un tuo documento di riconoscimento rilasciato dall'autorità**, inserire **i dati di una carta di credito** o **scattare una foto di te stesso (selfie)**.
Scopri di più sul requisito di verifica dell'età."

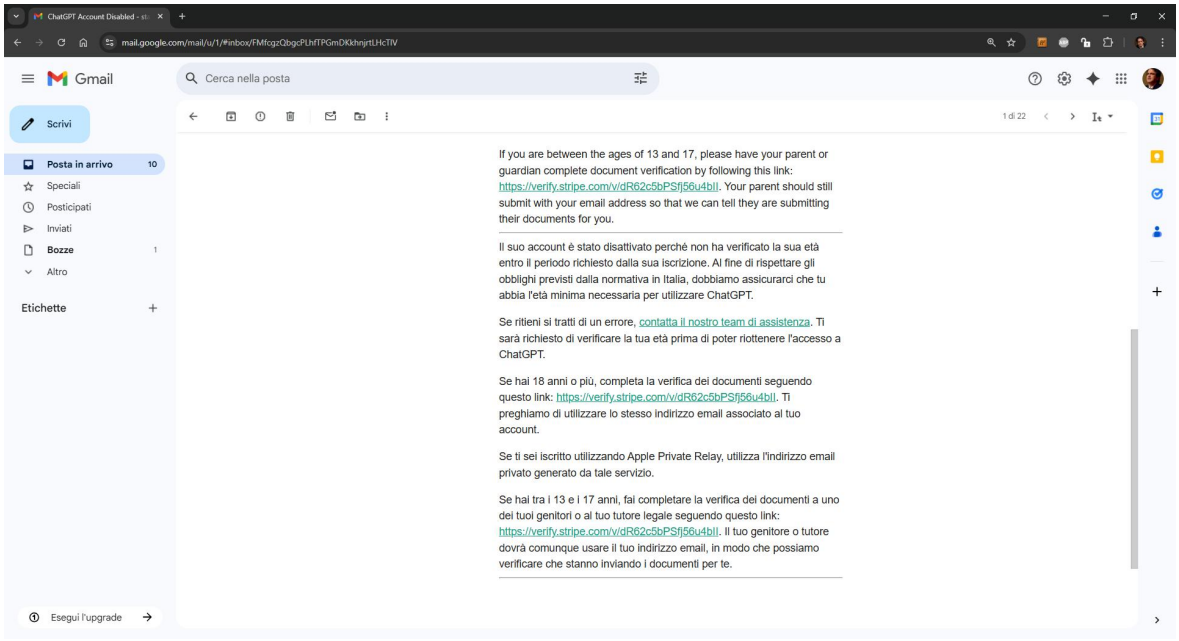
Nota

Si noti il passaggio chiave che rivela la natura **sproporzionata** della richiesta:

"Questi includono la possibilità di caricare un tuo **documento di riconoscimento** rilasciato dall'autorità, inserire i **dati di una carta di credito** o scattare una foto di te stesso (***selfie***)."

È fondamentale evidenziare che tali opzioni di acquisizione dei dati biometrici non costituiscono una "**possibilità**" discrezionale per l'utente, bensì di fatto un **obbligo**, in quanto il mancato completamento della procedura di verifica comporta la **disabilitazione dell'account**, come ben noto e illustrato nell'Allegato 2.





Allegato 2: Screenshots. Schermata notifica disabilitazione account

- Testo in Allegato 2 da OpenAI <noreply@tm.openai.com rispondi a: support@openai.com, data: 2 ago 2025, 16:16 (disabilitazione account):

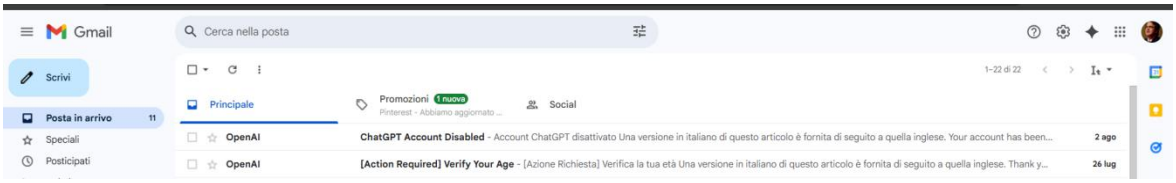
"Il suo account è stato **disattivato** perché **non ha verificato la sua età** entro il periodo richiesto dalla sua iscrizione. Al fine di rispettare gli obblighi previsti dalla normativa in Italia, dobbiamo assicurarci che tu abbia l'età minima necessaria per utilizzare ChatGPT.
Se ritieni si tratti di un errore, contatta il nostro team di assistenza. Ti sarà richiesto di verificare la tua età prima di poter riottenere l'accesso a ChatGPT.
Se hai 18 anni o più, completa la verifica dei documenti seguendo questo link: https://verify.stripe.com/v/dR62c5bPSfj56u4bII. Ti preghiamo di utilizzare lo stesso indirizzo email associato al tuo account.
Se ti sei iscritto utilizzando Apple Private Relay, utilizza l'indirizzo email privato generato da tale servizio.
Se hai tra i 13 e i 17 anni, fai completare la verifica dei documenti a uno dei tuoi genitori o al tuo tutore legale seguendo questo link: https://verify.stripe.com/v/dR62c5bPSfj56u4bII. Il tuo genitore o tutore

dovrà comunque usare il tuo indirizzo email, in modo che possiamo verificare che stanno inviando i documenti per te.”

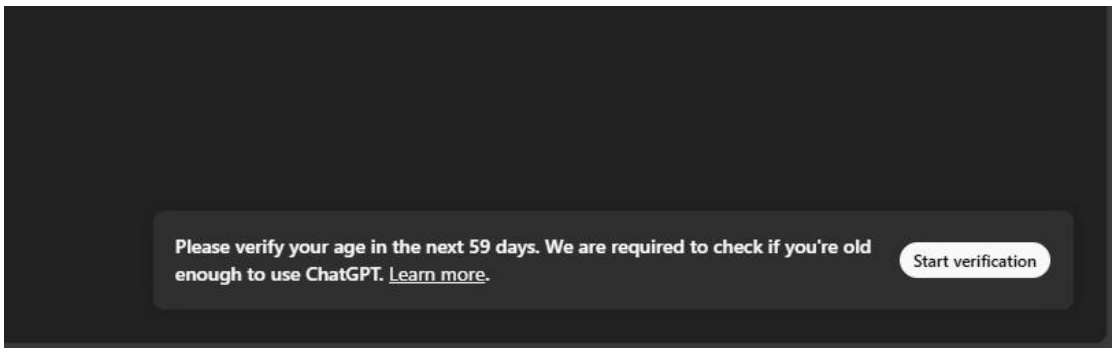
Nota sul link a Stripe Identity

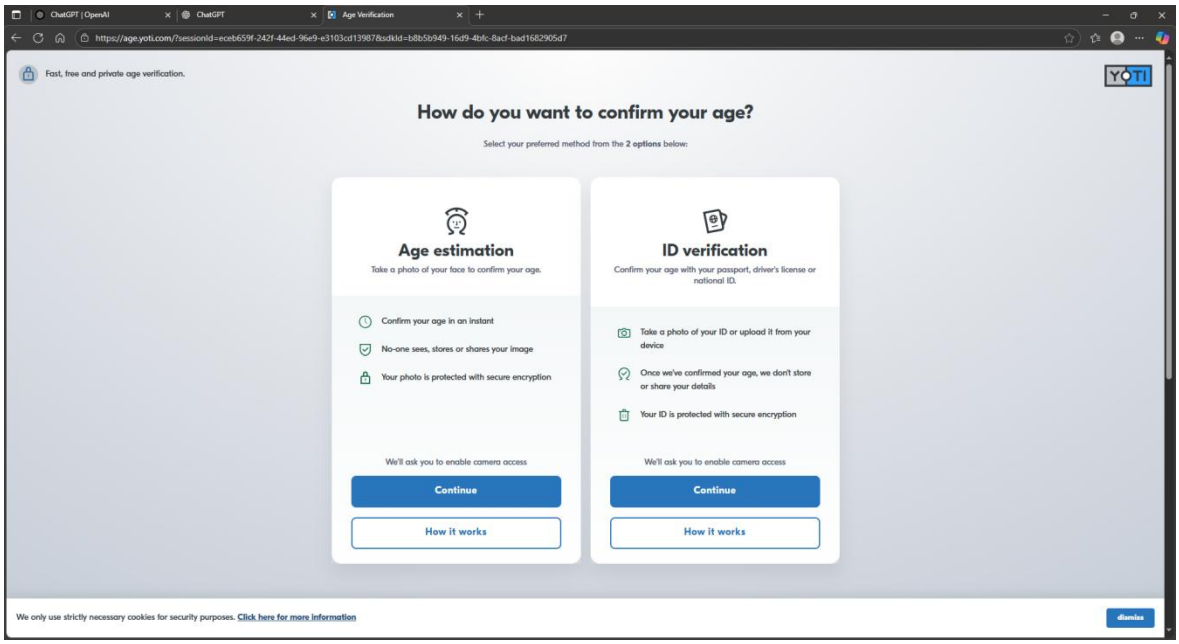
Si noti come, in alternativa, l'utente venga **redirezionato alla società Stripe Identity** per la “verifica” tramite caricamento di **documenti personali**, come evidenziato nel seguente estratto dall'email:

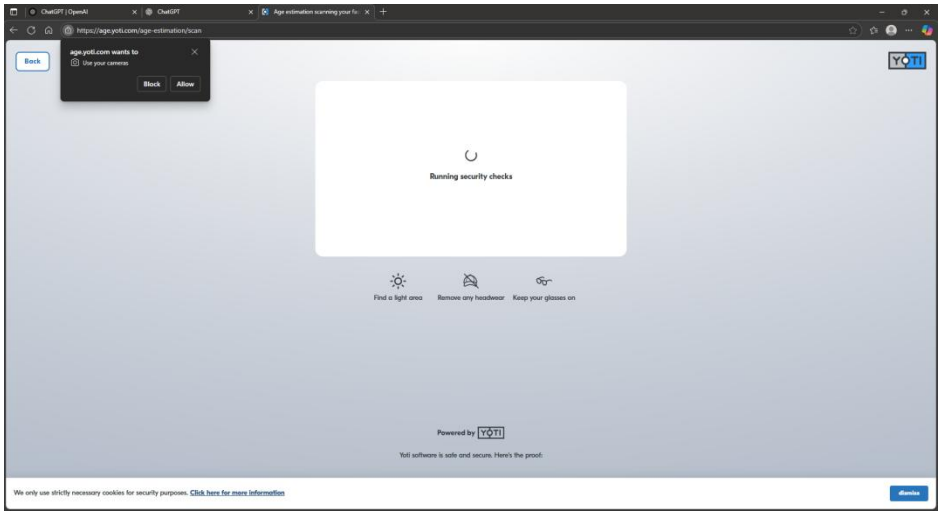
> ***"Se hai 18 anni o più, completa la verifica dei documenti seguendo questo link: https://verify.stripe.com/v/dR62c5bPSfj56u4bII."***

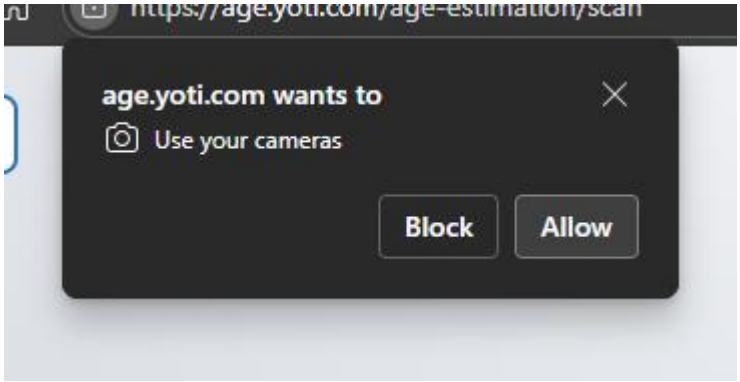


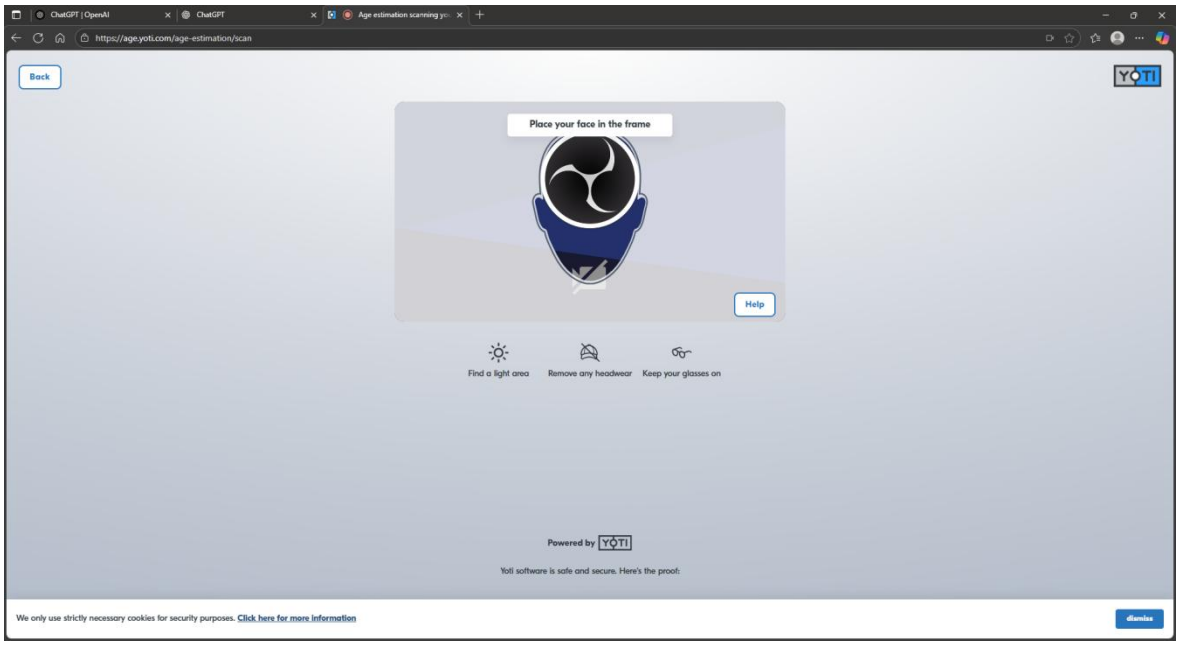
Allegato 3: Screenshot che mostra le comunicazioni di avviso e la successiva disabilitazione dell'account a seguito del mancato completamento della procedura di “***verifica dell'età***”, che include l'**invio di documenti personali e/o dati biometrici**. Le date delle comunicazioni sono: **Avviso di chiusura account** (26/07/2025) e **Disabilitazione account** (02/08/2025).




ChatGPT | OpenAI
ChatGPT
Age Verification
https://age.yoti.com/?sessionId=eceb659f-242f-44ed-96e9-e3103cd139878sdkId=b8b5b949-16d9-4bfc-8acf-bad1682905d7
Fast, free and private age verification.
YOTI
How do you want to confirm your age?
Select your preferred method from the 2 options below:
Age estimation
Take a photo of your face to confirm your age.
Confirm your age in an instant
No-one sees, stores or shares your image
Your photo is protected with secure encryption
We'll ask you to enable camera access
Continue
How it works
ID verification
Confirm your age with your passport, driver's license or national ID.
Take a photo of your ID or upload it from your device
Once we've confirmed your age, we don't store or share your details
Your ID is protected with secure encryption
We'll ask you to enable camera access
Continue
How it works
We only use strictly necessary cookies for security purposes. Click here for more information
dismiss


https://age.yoti.com/age-estimation/scan
Back
age.yoti.com wants to
Use your cameras
Block
Allow
YOTI
Running security checks
Find a light area
Remove any headwear
Keep your glasses on
Powered by YOTI
Yoti software is safe and secure. Here's the proof:
We only use strictly necessary cookies for security purposes. Click here for more information
dismiss





Allegato 4: Screenshots relativi a raccolta dati biometrici e possibile upload documento personale.

Conclusione e quadro d'insieme

La sequenza documentale allegata evidenzia un quadro di gravi violazioni sistemiche: la prassi di OpenAI di **imporre la raccolta di dati biometrici**, documenti personali e dati di pagamento, con il pretesto della "*verifica dell'età*", è **sproporzionata e illecita**, violando i principi del GDPR e compromettendo la sicurezza digitale, i diritti degli utenti e la sovranità digitale nazionale.
Si richiede a Codesta Autorità un intervento urgente per accertare le violazioni,

ordinare la cessazione delle pratiche illecite e adottare misure correttive, tutelando i diritti degli interessati e riaffermando il valore della **sovranità digitale**.

Assunzione di Responsabilità e Consenso al Trattamento dei Dati Personali

Il sottoscritto,
Prof. Tommaso Gastaldi, afferente al Dipartimento di Statistica e Informatica, Sapienza Università di Roma (email: tommaso.gastaldi@uniroma1.it),

presenta il presente esposto a **titolo personale**, precisando che l'istituzione di appartenenza è estranea ai contenuti e alle dichiarazioni ivi contenute.

Autorizza il Garante per la Protezione dei Dati Personali a trattare i dati personali forniti e il contenuto dell'esposto per le finalità istituzionali, ai sensi del D.Lgs. 196/2003 e del Regolamento (UE) 2016/679, in modo libero, informato e specifico, sollevando il Garante da ulteriori adempimenti autorizzativi. Il trattamento avverrà nel rispetto della normativa vigente, garantendo riservatezza e tutela dei diritti dell'interessato.

Con osservanza,

Documento trasmesso via PEC ai sensi dell'art. 65 del D.Lgs. 82/2005 (CAD)

Roma, 3 agosto 2025
Prof. Tommaso Gastaldi
Email: tommaso.gastaldi@gmail.com
Tel: +39 327 234 7610
PEC: tommaso.gastaldi@pec.it
