tinexta
defence

Persona: il "guardiano" delle identità.

#TinextaDefenceBusiness

Malware Lab

Our Malware Lab

Tinexta Defence Malware Lab daily performs dissection of malware with the aim of timely understanding the technological evolutions of attacks, consolidating the knowledge of necessary to make more effective and faster the process of incidents responding, contributing to spreading information about emerging threats into the expert's community and among its clients.

Malware Lab analysts are continuously engaged in searching and experimenting new analysis tools, for increasing accuracy and scope of action with regard to the proliferation of new evasion and anti-analysis techniques adopted by malware.

The Malware Lab is also committed to the development of proprietary tools for malware analysis and supporting the management and response of incidents.

Besides malware analysis, Malware Lab ideated and implemented an automatic process of extraction of **Indicators of Compromise (IOC)** that is daily run on dozens of new malwares, intercepted in the wide for populating our Knowledge Base.

Corrado Aaron Visaggio

Group Chief Scientist Officer & Malware Lab Director

a.visaggio@defencetech.it

Autori del report:

- Malware Lab: Ciriello Alberico, Gatto Emanuele
- AI4Cyber: Sorgente Simona
- Compliance: Lorusso Giorgia

Summary

1. Executive Summary 04

2. Cosa è successo 06

2.1 Il punto di partenza: Shodan 06
2.2 Codice esposto 06
2.3 Contenuto del codice 06
2.4 Double-check: verifica tecnica (24 febbraio 2026) 08

3. Chi usa Persona in Italia e in Europa 13

3.1 Clienti diretti ad alta visibilità 13
3.2 Clienti europei e integrazioni enterprise 14
3.3 Integrazione middleware: Persona è invisibile 15
3.4 Verifica database italiana: CIE e Codice Fiscale 16
3.5 La situazione per gli utenti italiani 16

4. Implicazioni legali 17

4.1 GDPR: i problemi concreti 17
4.2 AI Act: pratiche vietate? 19
4.3 Il Garante italiano: che può fare 19
4.4 BIPA: il precedente americano come leva di compliance globale 20

5. OpenAI: dichiarazioni e ambiguità 21

5.1 L'accordo OpenAI-Pentagono: contesto geopolitico 22

6. Domande aperte 23

7. Considerazioni finali 24

8. Fonti 26

1. Executive Summary

Persona[1] è una piattaforma cloud-based che fornisce soluzioni per la verifica dell'identità digitale. Da quando è stata fondata nel 2018, è diventata un fornitore importante di servizi Know Your Customer (KYC) e Know Your Business (KYB) per importanti piattaforme tech, quali ad esempio **OpenAI**, **Roblox**, **Reddit**, **Discord**, **LinkedIn**.

Il report è basato sulla ricerca originale pubblicata il 16 febbraio 2026 da vmfunc, MDL e Dziurwa su vmfunc.re/blog/persona. I tre gruppi di ricercatori hanno fatto delle scoperte importanti:

- Un'istanza Google Cloud dedicata a OpenAI openai-watchlistdb.withpersona.com è attiva da **novembre 2023**, 18 mesi prima di qualsiasi disclosure pubblica da parte di OpenAI sui requisiti di verifica.

- Su un deployment governativo (FedRAMP) della stessa piattaforma, **53 MB di codice TypeScript** erano accessibili senza autenticazione via source map JavaScript.

- Il codice estratto rivela: ricerca di corrispondenze tra i volti degli utenti con fotografie di politici; l'invio di Suspicious Activity Report (SAR) al FinCEN (Tesoro USA) oppure di Suspicious Transaction Report (STR) al Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), taggati con codici di programmi d'intelligence; mantenimento in database di dati biometrici fino a 3 anni ed esecuzione di 269 controlli distinti per ogni utente.

- La stessa azienda opera per utenti "consumer" (ad esempio, sulla verifica del volto per ChatGPT), per clienti enterprise (effettuando KYC e KYB) e, a quanto pare, per istituzioni governative.

[1] https://withpersona.com/

Da verifiche tecniche condotte il 24 febbraio 2026, il deployment di ONYX è stato **completamente rimosso** (il DNS non risolve più). La piattaforma governativa, quindi, è ora protetta da Google Cloud Platform Identity-Aware Proxy (GCP IAP) e l'infrastruttura OpenAI "watchlistdb" è **ancora attiva**.

Inoltre, approfondendo la documentazione pubblica sul sito web di Persona, sono state trovate delle funzionalità applicabili anche per clienti italiani, quali la "Database Verification" che offre la possibilità di verificare specifici attributi di un individuo contro database di istituzioni italiane.

Questo però fa sorgere più di un dubbio: c'è modo di verificare se queste funzionalità lasciano ed elaborano i dati solo in Italia? Vi è modo di accedere ai dati di cittadini italiani dagli Stati Uniti? I dubbi rimangono ed è anche lecito porsi delle domande.

Il CEO di Persona, Rick Song, ha risposto in buona fede e si è impegnato a rispondere per iscritto alle domande dei ricercatori. Ha dichiarato che "ONYX" è il nome del Pokémon preferito di un collega e che Persona **oggi non lavora con nessuna agenzia federale**[2].

[2] https://piunikaweb.com/2026/02/22/persona-ceo-releases-email-chain-vmfunc/

2. Cosa è successo

2.1 Il punto di partenza: Shodan

Tutto è partito da una ricerca su Shodan per analizzare l'infrastruttura di Persona. Su un IP di Google Cloud Platform (34.49.93.177) a Kansas City (USA), i ricercatori trovano due hostname:

openai-watchlistdb.withpersona.com
openai-watchlistdb-testing.withpersona.com

Su questa macchina è attiva un'istanza GCP isolata, dedicata. I log di Certificate Transparency mostrano che è attiva dal **16 novembre 2023**.

OpenAI ha iniziato a menzionare la raccolta biometrica nella Privacy Policy solo il 4 novembre 2024. Ha poi comunicato pubblicamente i requisiti di verifica per accedere ai modelli avanzati solo nel 2025, nonostante il watchlist screening fosse già attivo ben **18 mesi prima**.

2.2 Codice esposto

Sul portale governativo app.onyx.withpersona-gov.com, il build tool **Vite** stava servendo le source map JavaScript senza autenticazione. Le source map, quando compilate con sourcesContent: true, incorporano il codice TypeScript originale nel file .map.

Si tratta di 53 MB totali di file TypeScript su una piattaforma con certificazione **FedRAMP** (Federal Risk and Authorization Management Program).

2.3 Contenuto del codice

Modulo per inviare report al Tesoro americano: la piattaforma ha un modulo nativo per inviare Suspicious Activity Reports (SAR) direttamente al Tesoro americano. Non un'integrazione esterna: c'è un tasto "Send to FinCEN" con ciclo di vita completo (draft -> validate -> file -> accepted/rejected).

Modulo per inviare report al Tesoro canadese: analogamente esiste lo stesso modulo per il Canada, i Suspicious Transaction Report (STR) possono essere taggati in progetti relativi all' intelligence:

```
Project ANTON
Project ATHENA
Project CHAMELEON
Project GUARDIAN
Project LEGION
Project PROTECT
Project SHADOW
```

Questi sono programmi reali del Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Quando avviene una segnalazione da parte di utenti, queste vengono associate alle operazioni di intelligence sopracitate.

Modulo per riconoscimento facciale Politically Exposed Person (PEP): il selfie effettuato e caricato su una piattaforma associata ai servizi di Persona, viene confrontato con foto di politici, Capi di Stato e loro familiari (4 classi di PEP). Ad esso, poi, viene associato un punteggio di similarità: Low / Medium / High. Le foto di riferimento provengono da Wikidata.

Modulo per verifiche su ogni utente: il numero di verifiche applicabili è 269, di seguito degli esempi:

- SelfieSuspiciousEntityDetection: classifica i volti in "sospetti" senza specificare i criteri adottati.
- SelfieExperimentalModelDetection: esecuzione di modelli ML sperimentali, senza avere visibilità del nome, sulla biometria.
- SelfiePublicFigureDetection: verifica della somiglianza con personaggi pubblici noti.
- Lookup nel database SSA dei deceduti (USA).
- Analisi metadati PDF dei documenti caricati.
- Screening crypto via Chainalysis con re-screening automatico periodico.

Liste di tracciamento: vi sono 13 tipologie di liste che includono IP, browser fingerprint, device fingerprint, e-mail, numero di telefono, geolocalizzazione e una lista di volti che vengono conservati massimo per 3 anni.

Il deployment ONYX: ONYX è Apparso il 4 febbraio 2026, 12 giorni prima della pubblicazione. Ha la propria istanza GCP, namespace Kubernetes (persona-onyx) e certificato wildcard. Il nome coincide con Fivecast ONYX, uno strumento di sorveglianza acquistato dall'ICE (US Immigration and Custom Enforcement) per **$4,2 milioni**. Il codice estratto, però, non contiene riferimenti diretti a Fivecast o ICE.

2.4 Double-check: verifica tecnica (24 febbraio 2026)

È stata condotta una verifica tecnica di tutta l'infrastruttura menzionata nel blog originale, eseguendo DNS resolution, HTTP probing, analisi dei certificati TLS e interrogazione dei Certificate Transparency (CT) logs. Tutti i test sono stati condotti il **24 febbraio 2026** (8 giorni dopo la pubblicazione originale).

2.4.1 Deployment ONYX completamente rimosso

Questo è il risultato più significativo della verifica.

Tutti i sottodomini del deployment ONYX non risolvono più a livello DNS:

```
onyx.withpersona-gov.com          -> NXDOMAIN
app.onyx.withpersona-gov.com      -> NXDOMAIN
admin.onyx.withpersona-gov.com    -> NXDOMAIN
inquiry.onyx.withpersona-gov.com  -> NXDOMAIN
```

I certificati emessi il 4 e 5 febbraio 2026 risultano ancora nei CT logs (validi fino a maggio 2026), ma l'infrastruttura sottostante non è più visibile e accessibile da Internet. L'IP 34.10.180.174, inoltre, non è più associato ad alcun hostname di Persona.

Questo significa che le source map (i 53 MB di codice TypeScript) **non sono più accessibili**. Persona ha rimosso l'intero deployment piuttosto che semplicemente chiudere le source map. L'archiviazione dei ricercatori originali resta, quindi, l'unica copia nota.

2.4.2 GCP IAP aggiunto alla piattaforma governativa

La piattaforma governativa withpersona-gov.com e app.withpersona-gov.com sono ora protette da Google Cloud Platform Identity-Aware Proxy (GCP IAP). Ogni richiesta non autenticata riceve un redirect a accounts.google.com per autenticazione OAuth. Questa è una misura di sicurezza non presente al momento della ricerca originale.

Anche il path /vite-dev/ che serviva le source map è ora verificato da IAP. Per accedervi sarebbe necessaria un'autenticazione Google con permessi specifici.

La domanda sorge spontanea: **perché prima non c'erano questi controlli?** La protezione IAP è un controllo basilare per endpoint GCP. La sua assenza su una piattaforma FedRAMP è rilevante per la qualità dell'assessment di sicurezza.

2.4.3 openai-watchlistdb: ancora attivo

```
openai-watchlistdb.withpersona.com         → 34.49.93.177 (GCP)
openai-watchlistdb-testing.withpersona.com → 34.49.93.177 (GCP)

$ curl https://openai-watchlistdb.withpersona.com/
HTTP/2 404 | "fault filter abort" | via: 1.1 google

Certificato TLS:
  CN = openai-watchlistdb.withpersona.com
  Issuer: Google Trust Services, WR3
  Valido: 24 gen 2026 → 24 apr 2026
  SAN: openai-watchlistdb.withpersona.com,
       openai-watchlistdb-testing.withpersona.com
```

L'infrastruttura dedicata OpenAI è identica a quanto documentato nell'articolo originale. È isolata dalla rete Cloudflare, risponde con fault filter abort (Envoy proxy) e il certificato ruota regolarmente da novembre 2023. Il servizio di watchlist screening è pienamente operativo.

2.4.4 Staging watchlistdb: ancora esposto

```
staging-watchlistdb.withpersona-staging.com → 34.49.208.72 (GCP)
HTTP/2 404 | "fault filter abort"
```

L'ambiente di staging del watchlist screening è ancora attivo e raggiungibile. Restituisce la stessa risposta Envoy ed ha un IP GCP diverso.

2.4.5 security.txt: aggiornato post-pubblicazione

Nella ricerca originale era stato notato che il file security.txt del deployment ONYX era scaduto il 1º novembre 2025, ma è stato successivamente **aggiornato**:

```
Contact: mailto:security@withpersona.com
Expires: 2027-02-17T08:00:00.000Z
Preferred-Languages: en
```

La data di scadenza è stata portata al 17 febbraio 2027, esattamente un anno dopo la pubblicazione del blog. Il file security.txt sulla piattaforma governativa non è verificabile dall'esterno (restituisce Invalid IAP credentials: empty token).

2.4.6 Migrazione infrastrutturale Cloudflare FL1 -> FL2

Dalla **status page** di Persona (status.withpersona.com), è possibile estrarre un annuncio di manutenzione programmata per il **25 febbraio 2026** (il giorno dopo questa verifica):

"During this window, Persona will be working with Cloudflare to migrate our production network ingress from the FL1 architecture to the FL2 architecture. […] The FL2 architecture has been running in parallel with our existing FL1 setup for several weeks without issues."

FL2 è un'architettura Cloudflare di nuova generazione con routing più performante e feature di sicurezza aggiuntive.

2.4.7 Regione europea “DE” confermata

Durante un incidente avvenuto il 4 febbraio 2026 (lo stesso giorno della prima emissione del certificato ONYX), Persona ha segnalato nella status page: *“Functionality in DE region has been restored. We are working to restore full functionality in US region.”*

Persona gestisce una regione di elaborazione dati europea denominata **“DE1”** (Germania). Questo è rilevante poiché i dati biometrici di utenti europei, inclusi quelli italiani, **potrebbero** almeno transitare in questa regione. Purtroppo, non vi è modo di confermare ma è possibile solo fare supposizioni.

2.4.8 Connessione con Palantir

Open Rights Group ha reso pubblica un’informazione non presente nel blog originale: il principale investitore di Persona (tramite Founders Fund) è **Peter Thiel**, cofondatore di **Palantir** (l’azienda che fornisce strumenti analitici a ICE e al Ministero della Difesa israeliano).

2.4.9 Discord si ritira

Dopo la pubblicazione del report, Discord ha dichiarato che non utilizzerà Persona per la verifica dell’età e che era in sperimentazione nel mercato UK.

2.4.10 Anthropic e Groqcloud non menzionati nel blog

La lista pubblica dei subprocessor (aggiornata all’8 settembre 2025) include due piattaforme importanti non discusse nel blog originale: **Anthropic** e **Groqcloud**. Entrambe si occuperebbero di *“Data Extraction and Analysis”*, la stessa categoria di OpenAI. La loro inclusione suggerirebbe che Persona utilizza tre diversi provider di AI generativa per l’elaborazione dei documenti e l’estrazione dei dati. Menzione importante dovrebbe andare anche a **Resistant AI**, una società specializzata in rilevamento di frodi documentali basato su ML, che si occuperebbe di *“Document Analysis”*.

Nessuno dei subprocessor presente nell’elenco risiede nell’UE. Tutti i dati degli utenti italiani, quindi, potrebbero essere elaborati in infrastrutture statunitensi.

2.4.11 Riepilogo double-check

Asset	Stato pre-blog (16 feb)	Stato attuale (24 feb)	Cambiamento
ONYX (app.onyx.withpersona-gov.com)	Attivo, source map esposte	**DNS rimosso completamente**	☑ Rimediato
Source map /vite-dev/	Accessibili senza auth	**Dietro GCP IAP**	☑ Rimediato
withpersona-gov.com	Accessibile direttamente	**Dietro GCP IAP**	☑ Rimediato
openai-watchlistdb	IP esposto	**Invariato**	⚠
staging-watchlistdb	IP esposto	**Invariato**	⚠
security.txt (prod)	Scaduto l'11-01-2025 su ONYX	**Aggiornato al 17-02-2027**	☑ Aggiornato
SAR come servizio	Documentato nel codice	**Confermato nella status page**	🔍 Nuovo
Regione DE/EU	Non menzionata nel blog	**Confermata dalla status page**	🔍 Nuovo
Groqcloud subprocessor	Non menzionato	**Presente nella lista ufficiale**	🔍 Nuovo

3. Chi usa Persona in Italia e in Europa

Questo è un punto rilevante poiché Persona non è utilizzato solo da OpenAI in Europa, ma anche da altri servizi. Al momento della pubblicazione del report, i clienti sono confermati nelle seguenti sezioni.

3.1 Clienti diretti ad alta visibilità

Piattaforma	Uso	Rilevanza per utenti italiani
ChatGPT	Verifica dell'identità	Alta – accesso a GPT-4/5 API
Roblox	Verifica dell'età	Alta – milioni di minorenni italiani
Reddit	Verifica dell'età in UK per Online Safety Act (luglio 2025)	Media – Possibile espansione in UE
LinkedIn	Verifica identità con documento d'identità (procedura volontaria)	Media
Discord	Sperimentazione UK, poi ritirato	Bassa (per ora)
VRChat	Verifica dell'età (procedura volontaria)	Bassa

3.2 Clienti europei e integrazioni enterprise

È stato identificato un ecosistema di clienti molto ampio, in molti casi invisibile all'utente finale, che operano in Europa:

Asset	Settore	Paese	Tipo di integrazione	Fonte
Outkept	Cybersecurity B2B	Belgio	KYB (Know Your Business) e verifica degli utenti su documenti d'identità	Privacy Policy
GetYourGuide	Viaggi	Germania	KYB (Know Your Business) per operatori turistici, KYC (Know Your Customer) e informazioni su IP, device, geolocalizzazione	Persona customer
WeTravel	Pagamenti e Viaggi	Paesi Bassi	KYB (Know Your Business) e KYC (Know Your Customer)	Persona customer
Discogs	E-commerce Musica	USA/globale[3]	KYB (Know Your Business). Verifiche sui venditori, collezione e conservazione di loro informazioni	Persona customer
Lendfoundry	Lending / fintech	USA/globale	KYC (Know Your Customer) e verifica documenti per evitare frodi finanziarie	Lendfoundry blog
Yardstik	Assunzioni e Risorse umane	USA	Verifica identità dedicato alle assunzioni	Yardstik blog
Cisco Duo (Two Five Labs)	Identity and Access Management / Cybersecurity	USA	Verifica identità dedicato ad Help Desk aziendali	Duo documentation
Phound	VoIP / Telecomunicazioni	USA	KYC (Know Your Customer) per utenti VoIP	Official page
101domain	Gestione domini	USA	Verifica identità registranti	Identity verification
Character.ai	LLM	USA	Verifica dell'età tramite verifica facciale e dei documenti d'identità	Help center

[3] Ha una sede europea

Nota: alcune fonti potrebbero non essere più raggiungibili dopo la pubblicazione del report per via di possibili rimozioni dei riferimenti a Persona.

Particolarmente rilevante è Character.ai, il quale, ha implementato un sistema a cascata in cui gli utenti sospettati di essere minorenni vengono prima valutati su base comportamentale, poi con foto del volto e infine tramite documento d'identità, tutto tramite Persona. Questo modello probabilmente potrebbe essere oggetto di future regolamentazioni sotto l'AI Act dell'UE.

3.3 Integrazione middleware: Persona è invisibile

Nella maggior parte dei casi sopracitati, Persona non è visibile all'utente finale. L'utente interagisce esclusivamente con l'interfaccia della piattaforma cliente (Roblox, ChatGPT, Character.ai) e il flusso di verifica appare come una funzionalità nativa del servizio. In nessun momento del processo viene tipicamente comunicato che i dati biometrici – selfie, documento d'identità, metadati del dispositivo – vengono trasmessi a un soggetto terzo per l'elaborazione.

Questo modello di integrazione ha implicazioni dirette ai sensi del GDPR. L'informativa ex artt. 13-14 del Regolamento richiede che l'interessato sia informato dell'identità di ogni responsabile del trattamento e delle categorie di destinatari dei dati personali, inclusi i subprocessor.

Persona, in qualità di responsabile del trattamento ai sensi dell'art. 28, dovrebbe essere esplicitamente menzionata nelle informative privacy di ciascun titolare. Una verifica a campione sulle informative privacy di alcuni dei clienti elencati nella sezione precedente evidenzia che il riferimento a Persona come responsabile del trattamento non è sempre presente, o è limitato a un generico rinvio a "fornitori di servizi di verifica dell'identità" senza indicazione del nome, della sede e delle categorie di dati trattati. Questa opacità è particolarmente critica nel caso di dati biometrici, che rientrano tra le categorie particolari ex art. 9 GDPR e richiedono un livello di trasparenza rafforzato. Il rischio concreto è che un utente italiano che effettua una verifica dell'età su Roblox o una verifica dell'identità su LinkedIn non sappia che i propri dati biometrici vengono elaborati da un'azienda statunitense, tramite subprocessor anch'essi statunitensi, con tempi di conservazione che possono estendersi ben oltre quanto comunicato nell'informativa del titolare.

3.4 Verifica database italiana: CIE e Codice Fiscale

La documentazione tecnica di Persona (help.withpersona.com) descrive un modulo specifico: **Database Verification (Italy)**. Questo modulo:

- Richiede all'utente input obbligatori: **nome, data di nascita, documento d'identità nazionale** (CIE o Codice Fiscale), **indirizzo**
- Verifica questi dati contro "database autoritativi italiani" (non specificati quali, potrebbe trattarsi di Anagrafe, Agenzia delle Entrate, o fornitori terzi)
- È disponibile sui piani Essential, Growth e Enterprise (non sullo starter gratuito)
- Il piano Enterprise include configurazioni avanzate: verifica telefono/e-mail, requisiti di match personalizzati

Questo significa che Persona ha, o afferma di avere, **accesso diretto a database governativi italiani** per la validazione dell'identità. La CIE (Carta d'Identità Elettronica) è il documento digitale italiano per eccellenza. Che un'azienda statunitense, finanziata da Founders Fund, possa verificare i numeri CIE dei cittadini italiani contro database autoritativi solleva domande sulla catena di elaborazione dei dati che nessuna informativa privacy espone.

3.5 La situazione per gli utenti italiani

Per gli utenti italiani la piattaforma più rilevante è Roblox, la quale ha adottato Persona globalmente a gennaio 2026. Genitori e minori italiani che verificano l'età su Roblox stanno passando per questo sistema: la foto del volto del minore verrebbe elaborata da LLM (OpenAI, Anthropic, Groqcloud), confrontata con database biometrici e mantenuta per un determinato periodo.

Discord, molto diffuso in Italia, ha annunciato una verifica età globale per inizio 2026. Sebbene si sia ritirata dall'uso di Persona (per ora), utilizzerà sistemi analoghi. La tendenza europea di verifica dell'età (EU Digital Services Act, UK Online Safety Act, AI Act) spingerà più piattaforme a soluzioni KYC nelle prossime settimane.

Una **questione critica** riguarda quasi tutti i subprocessor di Persona che risiedono negli USA, poiché non esiste un subprocessor in UE. Anche se i dati venissero inizialmente elaborati nella regione DE (Germania), potrebbero essere poi inoltrati a OpenAI (USA), Anthropic (USA), Groqcloud (USA), e MongoDB Atlas (USA). Il percorso dei dati biometrici di un tredicenne italiano su Roblox potrebbe essere: dispositivo -> Cloudflare -> GCP (forse Germania, forse USA) -> OpenAI/Anthropic/Groqcloud (USA) -> MongoDB (USA).

4. Implicazioni legali

4.1 GDPR: i problemi concreti

I dati biometrici rientrano tra le categorie particolari di dati personali ai sensi dell'art. 9 GDPR e, come regola generale, il loro trattamento è vietato, salvo specifiche eccezioni previste dal Regolamento. Il consenso prestato in fase di registrazione a ChatGPT difficilmente può ritenersi conforme ai requisiti del GDPR, poiché potrebbe non essere:

- Libero, in quanto l'alternativa sarebbe non poter utilizzare il servizio;
- Specifico e granulare, poiché l'interessato non è messo nella condizione di conoscere nel dettaglio le modalità e l'estensione del trattamento (ad esempio l'esistenza di numerosi controlli o verifiche);
- Informato, se non viene chiaramente comunicato che l'immagine del volto può essere oggetto di confronto con quella di soggetti terzi, inclusi soggetti pubblici.

Di seguito si riportano i principali profili di criticità ai sensi del GDPR:

Art. 13-14 (Informativa): Gli interessati non risulterebbero informati circa il fatto che il selfie venga confrontato con database relativi a soggetti PEP, né circa l'esistenza di 269 controlli distinti effettuati sul dato. Non viene inoltre chiarito che i dati biometrici possono essere conservati fino a 3 anni (o, nel caso di documenti governativi, anche permanentemente). OpenAI indica una conservazione "fino a 1 anno", mentre il codice prevede un termine massimo di 3 anni: permane quindi un'incertezza circa l'effettivo periodo di retention. Infine, la presenza di tre diversi provider AI (OpenAI, Anthropic e Groqcloud) non risulta comunicata nelle informative standard.

Art. 22 (Decisioni automatizzate): L'accesso al servizio viene negato mediante un processo interamente automatizzato, in assenza di intervento umano. Non risultano fornite spiegazioni in merito ai criteri decisionali applicati, né è previsto un meccanismo di riesame o di impugnazione della decisione. La community di OpenAI documenta inoltre casi di utenti che, pur avendo inizialmente superato la verifica, vengono successivamente bloccati senza motivazione apparente.

Art. 44–49 (Trasferimenti internazionali): I dati biometrici di cittadini UE vengono trasferiti negli Stati Uniti. Sebbene Persona dichiari la presenza di una regione DE (Germania) per l'elaborazione iniziale, i oltre 20 sub-processor coinvolti risultano localizzati negli USA o in Canada, tra cui OpenAI (San Francisco), Anthropic (San Francisco), Groqcloud (San Jose), MongoDB Atlas (USA), Snowflake (USA), AWS (USA) ed Elasticsearch (USA). Il Data Privacy Framework UE-USA (2023) è attualmente in vigore quale meccanismo di adeguatezza, ma risulta già oggetto di contestazione. Max Schrems (noyb) ha più volte sostenuto che tale framework potrebbe essere invalidato dalla CGUE, come avvenuto in precedenza con il Safe Harbor (2015) e il Privacy Shield (2020).

Art. 5, par. 1, lett. c) ed e) (Principio di limitazione della conservazione e minimizzazione): Emergono tre diverse indicazioni in merito ai tempi di conservazione: 1 anno (secondo OpenAI), 3 anni (secondo il codice) e conservazione permanente per i documenti governativi. In assenza di chiarezza circa il periodo effettivo di retention, non risulta possibile verificare il rispetto del principio di minimizzazione e della limitazione della conservazione. La documentazione di Persona indica, nella sezione marketing, un termine di "7–14 giorni" per i dati biometrici; tuttavia, il codice evidenzia l'esistenza di una face list con retention massima di 3 anni e, per clienti operanti nel settore finanziario, periodi di conservazione che possono estendersi fino a 10 anni.

Art. 28 (Responsabile del trattamento): Persona opera quale responsabile del trattamento per conto di OpenAI, Roblox e altri titolari. Tuttavia, il modulo "Database Verification (Italy)", che prevede la verifica di CIE e Codice Fiscale rispetto a "database autoritativi italiani", comporta un trattamento diretto di dati governativi italiani. La catena di sub-responsabili (Persona -> OpenAI -> Groqcloud -> MongoDB) non risulta trasparente nei confronti dell'interessato. Ogni ulteriore passaggio nella filiera di trattamento determina un incremento del rischio di data breach e l'assoggettamento dei dati a ulteriori giurisdizioni.

4.2 AI Act: pratiche vietate?

L'AI Act, la cui applicazione sarà progressiva fino al 2026, vieta alcune pratiche di IA considerate inaccettabili, tra cui determinati sistemi di categorizzazione biometrica fondati su caratteristiche sensibili (art. 5). Un sistema come "Selfie-SuspiciousEntityDetection", che attribuisca la categoria di "sospetto" sulla base dell'immagine del volto secondo criteri non comunicati, potrebbe potenzialmente rientrare nell'ambito delle pratiche vietate, ove la classificazione implichi una categorizzazione biometrica o una valutazione automatizzata riconducibile alle ipotesi di cui all'art. 5.

I sistemi di identificazione biometrica remota sono qualificati come ad alto rischio ai sensi dell'Allegato III (in combinato disposto con gli artt. 6–7). In tali casi, i fornitori devono garantire, prima dell'immissione sul mercato o della messa in servizio nell'Unione, il rispetto dei requisiti previsti dal Regolamento, inclusi adeguati livelli di trasparenza, supervisione umana effettiva e documentata, nonché accuratezza e robustezza del sistema.

Il sistema a cascata adottato da Character.ai (analisi comportamentale -> selfie -> documento di identità) risulta particolarmente rilevante, in quanto combina profilazione comportamentale e trattamento biometrico in un unico flusso decisionale, con possibile intersezione sia con le pratiche vietate ex art. 5 sia con il regime dei sistemi ad alto rischio di cui agli artt. 6–7 e Allegato III.

4.3 Il Garante italiano: che può fare

Il Garante per la Protezione dei Dati Personali è già intervenuto nei confronti di OpenAI nel marzo 2023, disponendo una limitazione provvisoria del trattamento relativo a ChatGPT e richiedendo l'adozione di misure correttive.

Qualora il trattamento coinvolga interessati stabiliti in Italia, l'Autorità può esercitare i poteri previsti dagli artt. 55 e 58 GDPR, tra cui:

- avviare un'istruttoria d'ufficio;
- richiedere lo svolgimento o l'esibizione di una Data Protection Impact Assessment (DPIA), ove dovuta, sia al titolare sia al responsabile;
- verificare le modalità di accesso ai "database autoritativi italiani" nell'ambito del modulo di verifica CIE/Codice Fiscale;

- accertare la corretta designazione di Persona quale responsabile del trattamento ai sensi dell'art. 28 GDPR e la conformità dell'intera catena di sub-responsabili;
- adottare provvedimenti correttivi, inclusa la limitazione o il divieto del trattamento;
- irrogare sanzioni amministrative pecuniarie fino al 4% del fatturato mondiale annuo dell'impresa responsabile, nei casi previsti dall'art. 83 GDPR;
- attivare il meccanismo di cooperazione e coerenza con le altre autorità di controllo europee tramite l'European Data Protection Board (EDPB), ove ricorra un trattamento transfrontaliero.

La presenza di un modulo di verifica specificamente riferito all'Italia (CIE + Codice Fiscale) rafforza il collegamento territoriale con l'ordinamento italiano e può giustificare l'intervento dell'Autorità nazionale, ferma restando l'eventuale applicazione del meccanismo dello "sportello unico" in caso di trattamento transfrontaliero.

La base giuridica per un accertamento istruttorio potrebbe dunque sussistere; resta una valutazione discrezionale dell'Autorità l'eventuale apertura di un procedimento formale e le relative tempistiche.

4.4 BIPA: il precedente americano come leva di compliance globale

Il Biometric Information Privacy Act (BIPA) dello Stato dell'Illinois non è direttamente applicabile in Italia né nell'Unione europea. La sua rilevanza per il contesto europeo è tuttavia di natura indiretta e concreta, in quanto le conseguenze sanzionatorie sul mercato statunitense possono determinare modifiche architetturali e organizzative con effetti su scala globale.

Il BIPA richiede il previo consenso scritto e informato dell'interessato prima di qualsiasi raccolta di dati biometrici, unitamente alla comunicazione delle finalità del trattamento e del relativo periodo di conservazione. In caso di violazione, la normativa prevede danni statutari pari a 1.000 USD per violazione negligente e 5.000 USD per violazione dolosa o intenzionale, per ciascun singolo atto di raccolta.

Il contenzioso BIPA ha già prodotto conseguenze finanziarie rilevanti per piattaforme tecnologiche operanti su larga scala. Nel 2021, Meta ha concordato un settlement di 650 milioni di USD per la raccolta non autorizzata di dati biometrici tramite il sistema Tag Suggestions di Facebook. Nel 2023, Google ha definito un accordo da 100 milioni di USD relativo alla funzionalità di raggruppamento facciale di Google Photos. In entrambi i casi, le aziende hanno successivamente modificato le proprie policy biometriche a livello globale, non limitatamente alla giurisdizione dell'Illinois.

Qualora OpenAI raccolga dati biometrici tramite Persona anche con riferimento a utenti soggetti alla giurisdizione dell'Illinois — ipotesi plausibile considerata la scala dichiarata di "milioni" di verifiche mensili — l'esposizione potenziale è dell'ordine di miliardi di dollari. A tali livelli di rischio finanziario, le aziende tendono a uniformare le proprie pratiche verso lo standard più restrittivo piuttosto che mantenere architetture differenziate per giurisdizione. Modifiche quali la riduzione dei tempi di retention, la separazione dei flussi di dati per area geografica o l'introduzione di meccanismi di consenso granulare, se adottate in risposta al rischio BIPA, produrrebbero effetti diretti anche per gli utenti stabiliti nell'Unione europea.

Il BIPA rappresenta pertanto un fattore di pressione esterno che, pur originando da un ordinamento diverso, può accelerare l'adeguamento delle pratiche di trattamento biometrico anche nei confronti degli interessati europei.

5. OpenAI: dichiarazioni e ambiguità

Nel codice estratto dalle source map sono presenti due riferimenti significativi relativi a OpenAI.

Il file dashboard/hooks/useAgentConversationStream.ts implementa un assistente conversazionale in streaming, denominato "AskAI", destinato agli operatori della dashboard di Persona. Il modulo si interfaccia direttamente con api.openai.com e gestisce il ciclo completo degli eventi SSE (Server-Sent Events) del protocollo OpenAI: creazione della risposta, streaming del testo, completamento ed errore.

Il file lib/constants/externalIntegrationVendors.ts classifica OpenAI nella categoria ExternalIntegrationProductivityOpenAi, la medesima categoria assegnata a Slack e Zendesk. OpenAI non è dunque classificato nel codice come strumento di sorveglianza o di analisi dati, bensì come strumento di produttività per gli operatori.

Questa evidenza ridimensiona parzialmente l'ipotesi che OpenAI riceva flussi diretti di dati personali identificativi (PII) attraverso la piattaforma. Il codice, per quanto visibile, non mostra trasmissione di PII verso l'API OpenAI.

Tuttavia, il dato solleva una questione tecnica rilevante che il codice non risolve: il copilot AskAI opera sulla medesima piattaforma che gestisce Suspicious Activity Report, screening biometrico e riconoscimento facciale PEP. Non è documentato quale contesto sia accessibile all'assistente quando un operatore formula una richiesta durante la revisione di un caso. In un'architettura in cui l'assistente ha accesso al contesto della sessione operativa — ipotesi tecnicamente plausibile ma non confermata dal codice disponibile — le query degli operatori potrebbero contenere implicitamente riferimenti a dati sensibili relativi agli interessati in fase di valutazione. L'assenza di documentazione sulla segmentazione del contesto tra il copilot e i moduli di screening rappresenta un'area di indagine che meriterebbe chiarimento da parte di Persona.

5.1 L'accordo OpenAI–Pentagono: contesto geopolitico

Il 28 febbraio 2026, OpenAI ha formalizzato un accordo con il Dipartimento della Difesa statunitense per la fornitura di servizi di intelligenza artificiale alle reti classificate del Pentagono. L'accordo prevede tre limitazioni dichiarate: nessun impiego per sorveglianza di massa domestica, nessun sistema d'arma autonomo e nessun sistema di "credito sociale". OpenAI ha affermato che tali vincoli sarebbero ancorati alla legislazione vigente e non modificabili da eventuali future revisioni normative.

Questa decisione si inserisce in un contesto più ampio in cui il rapporto tra i principali fornitori di AI e le istituzioni governative statunitensi è in rapida evoluzione. Il punto rilevante per questo report non è l'accordo in sé, quanto la domanda che esso pone in combinazione con quanto emerso dall'analisi di Persona: OpenAI è simultaneamente subprocessor per la raccolta e l'elaborazione di dati biometrici di milioni di utenti civili (attraverso Persona) e fornitore di tecnologia AI per reti classificate del Dipartimento della Difesa.

Non vi è evidenza che i due ambiti siano connessi, ma non vi è neppure documentazione pubblica che ne attesti la separazione architetturale e organizzativa.

La raccolta biometrica tramite Persona risulta operativa dal novembre 2023, almeno 12 mesi prima di qualsiasi comunicazione pubblica da parte di OpenAI in merito ai requisiti di verifica dell'identità. Questa asimmetria temporale tra operatività e disclosure rafforza la necessità, già evidenziata nelle sezioni precedenti, di maggiore trasparenza sulla catena di trattamento dei dati e sulle garanzie di separazione tra i diversi ambiti operativi dell'azienda.

6. Domande aperte

Questo report apre a numerose domande e lascia diversi dubbi. Alcune questioni che riteniamo fondamentali per il contesto europeo sono:

1. **Qual è la vera retention biometrica?** OpenAI dice 1 anno, il codice dice 3 anni per le "face list", i documenti governativi "permanentemente", il marketing dice 7–14 giorni. Serve una risposta unica, verificabile, vincolante.
2. **Esiste una Data Protection Impact Assessment (DPIA) per gli utenti europei?** La raccolta biometrica di massa richiede una Data Protection Impact Assessment. È mai stata effettuata? È mai stata comunicata al Garante?
3. **Quali garanzie di separazione esistono** tra Persona e l'ambiente governativo statunitense?
4. **Cosa definisce un volto "sospetto"** in SelfieSuspiciousEntityDetection? Qual è il tasso di falsi positivi? Qual è il processo di revisione per chi viene rifiutato?
5. **Chi sono i clienti attuali di Persona?** Persona afferma di non avere contratti governativi federali oggi, ma FedRAMP esiste per un motivo. Quali agenzie stanno usando o valuteranno la piattaforma?
6. **A quali "database autoritativi italiani" accede il modulo Database Verification (Italy)?** Con quale base giuridica? Il Garante ne è informato?
7. **Quale ruolo specifico svolgono Anthropic e Groqcloud come subprocessor?** I dati biometrici transitano per tutti e tre i provider?
8. **La regione DE (Germania) è effettivamente utilizzata per i dati EU?** O è un'opzione disponibile ma non attiva per default? I dati elaborati nella regione DE vengono poi inoltrati ai subprocessor USA?
9. **Perché la protezione IAP non era attiva sulla piattaforma FedRAMP?** Questo fallimento infrastrutturale è stato oggetto di un incident report formale? L'assessment FedRAMP è stato rifatto dopo la scoperta?

7. Considerazioni finali

Questa vicenda ha diversi strati ed **il problema strutturale non è la sorveglianza in sé**. In un contesto in cui le piattaforme devono fronteggiare frodi, furti d'identità e finanziamenti al terrorismo, esistono ragioni legittime per l'implementazione e l'utilizzo di sistemi KYC. Tuttavia, il problema è che questi sistemi vengono applicati in modo opaco ad utenti che rimangono all'oscuro dell'operato che vi è dietro.

Uno scenario comune è il caricamento di un documento d'identità per l'iscrizione ai servizi forniti da LLM (ad esempio ChatGPT). La ragione per cui viene richiesto è la verifica dell'età, ma in quel momento si entra in un sistema che può classificarti come "entità sospetta" sulla base del volto, confrontare la propria foto con fotografie di politici ed inserire il profilo in liste biometriche che vengono controllate periodicamente.

Il paradosso FedRAMP sembra il punto più rilevante tecnicamente, poiché è un sistema certificato come sicuro. Eppure, qualcuno ha rilasciato in produzione una build di sviluppo, con le source map abilitate, su un endpoint pubblico e su una piattaforma governativa. La certificazione FedRAMP ha valutato l'architettura, non quella specifica configurazione Kubernetes. Questo dice qualcosa di importante sulla differenza tra compliance e sicurezza reale. Il fatto che dopo la pubblicazione Persona abbia **rimosso l'intero deployment ONYX e aggiunto GCP IAP**, conferma che il problema non era una svista, ma un'assenza di processi.

La risposta del CEO di Persona evidenzia un problema strutturale, non personale. Rick Song ha risposto rapidamente ai ricercatori, dichiarando che Persona non intrattiene rapporti contrattuali con agenzie federali statunitensi e che il nome "ONYX" non ha alcuna connessione con il prodotto omonimo di Fivecast. La disponibilità al dialogo è apprezzabile e non vi è ragione per dubitare della buona fede della risposta. Tuttavia, il punto rilevante non è se le dichiarazioni del CEO siano veritiere, ma il fatto che la veridicità stessa non sia verificabile in modo indipendente. Ad oggi non risultano pubblicati: audit di terze parti sull'effettiva separazione tra l'ambiente commerciale e quello governativo; documentazione tecnica sulla segmentazione dei flussi di dati biometrici per giurisdizione; né report di compliance FedRAMP aggiornati post-incidente che confermino l'avvenuta remediation.

In un contesto in cui una singola piattaforma gestisce simultaneamente verifiche biometriche per utenti consumer, clienti enterprise e – quantomeno fino a pochi giorni prima della disclosure – un deployment con caratteristiche governative, l'assenza di garanzie strutturali documentate e verificabili rappresenta una criticità indipendente dalla buona fede di qualsiasi dichiarazione.

L'elenco dei subprocessor è un altro dato preoccupante. Tre provider AI diversi (OpenAI, Anthropic, Groqcloud) elaborano i dati biometrici, e nessuno di loro risiede nell'UE. Ad essi si aggiungono molte altre aziende "tech" tutte con sede in USA. La regione DE (Germania) esiste ma è solo il punto di ingresso probabilmente: i dati, forse, vengono poi inoltrati oltreoceano. Per un utente italiano, il percorso dei propri dati biometrici attraversa potenzialmente 5-6 giurisdizioni e altrettanti provider cloud prima di tornare con un "verificato" o "rifiutato".

Il collegamento con Palantir/Thiel, emerso dopo la pubblicazione originale, non è una "pistola fumante" ma è un segnale di contesto. Il principale investitore di Persona è il cofondatore di Palantir, l'azienda che vende strumenti analitici all'ICE. Questo non prova niente, però sapere chi controlla i dati è estremamente rilevante.

Gli utenti italiani usano diversi servizi americani che richiedono verifiche, per cui l'impatto è difficile da calcolare. Un esempio è Roblox, che ha adottato Persona globalmente a gennaio 2026 per la verifica dell'età, quindi anche in Italia. Ciò significa che un ragazzo di 13 anni che vorrebbe accedere a determinate funzionalità di Roblox, caricherebbe il suo documento d'identità per essere elaborato da questo sistema. I suoi dati biometrici, probabilmente, verranno quindi elaborati su infrastrutture americane ed è ignoto per quanto tempo verranno conservati nei loro sistemi.

Il modulo Database Verification (Italy) aggiunge un ulteriore livello di opacità. Persona non solo raccoglie i dati biometrici, ma afferma di poter verificare CIE e Codice Fiscale contro "database autoritativi italiani", anche se non è chiaro quali siano. In ogni caso, un'azienda americana con investitori della Silicon Valley ha accesso diretto alla verifica dell'identità digitale italiana. Questa è una situazione opaca in cui il Garante dovrebbe investigare. I genitori italiani che hanno fatto la verifica dell'età del proprio figlio su Roblox probabilmente non sanno niente di tutto questo.

8. Fonti

8.1 Ricerca originale e risposte

- vmfunc.re/blog/persona – Ricerca originale (16 feb 2026)
- piunikaweb.com – Persona CEO releases email chain – Corrispondenza Rick Song / vmfunc

8.2 Copertura media e analisi

- malwarebytes.com – Age verification vendor Persona left frontend exposed – Discord si ritira da utilizzo di Persona
- openrightsgroup.org – Roblox, Reddit and Discord users compelled to use biometric ID backed by Peter Thiel – Connessione conFounders Fund e Palantir
- cybernews.com – Persona leak links age verification and federal surveillance – Dichiarazione CEO
- eff.org – ICE going on a surveillance shopping spree – Contesto ICE/Fivecast ONYX
- wikipedia.org – Persona (identity verification service) – Overview clienti aggiornata

8.3 Infrastruttura e documentazione Persona

- withpersona.com/legal/subprocessors – Lista subprocessor (aggiornata 8 set 2025)
- help.withpersona.com – Database Verification (Italy) – Modulo verifica CIE/Codice Fiscale
- status.withpersona.com – Status page
- crt.sh – openai-watchlistdb.withpersona.com – CT logs OpenAi
- crt.sh – onyx.withpersona-gov.com – CT logs ONYX

8.4 Normative

- GDPR – Regolamento UE 2016/679
- AI Act – Regolamento UE 2024/1689
- FedRAMP – marketplace.fedramp.gov/products/FR2405441061 – Autorizzazione Persona
- BIPA – Illinois Biometric Information Privacy Act (740 ILCS 14)

tinexta
defence

Next | Donexit | Foramil | Innodesi

Via Giacomo Peroni, 452 – 00131 Roma
tel. 06.45752720 – info@defencetech.it
www.tinextadefence.it

#TinextaDefenceBusiness