



noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienne
Autriche

CNIL
3 Place de Fontenoy
TSA80715
75334 PARIS CEDEX 07
FRANCE

Via le formulaire en ligne

Vienne, le 27.10.2026

N° de dossier *noyb* : C109-01

Plaignant :

[REDACTED]
né [REDACTED]
[REDACTED]

représenté en vertu de
l'article 80(1) RGPD

noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2, 1140 Vienne, Autriche

Partie défenderesse :

Scale AI, Inc.,
650 Townsend Street, San Francisco
États-Unis

Objet :

**La violation des articles 5(1)(c), 12(3), 15, 25(1) et
28(1) RGPD et de l'article 82 de la loi informatique et
libertés**

PLAINTÉ

1. REPRÉSENTATION

1. *noyb* – European Center for Digital Rights est une organisation à but non lucratif active dans le domaine de la protection des droits et libertés des personnes concernées, dont le siège social est situé à Goldschlagstraße 172/4/3/2, 1140 Vienne, Autriche, numéro d'enregistrement ZVR : 1354838270 (ci-après : "*noyb*") (**annexe 1**).
2. *noyb* représente le plaignant en vertu de l'Article 80(1) RGPD (**annexe 2**).

2. CONTEXTE

3. Le travail exécuté via des plateformes est un mode de travail qui concerne des centaines de millions de personnes, dont au moins 43 millions en Europe. Leur nombre a plus que doublé depuis 2022 et est appelé à augmenter de manière exponentielle (ci-après le « Platform Work »).¹
4. Le Platform Work inclut entre autres les coursiers, les chauffeurs dits « ubérisés » et, catégorie dont le nombre augmente particulièrement récemment : les annotateurs de données, travaillant à la modération et à l'entraînement des intelligences artificielles. Cette dernière catégorie fait l'objet de la présente plainte.
5. Le Platform Work soulève généralement une vulnérabilité particulière comparé à d'autres emplois. Premièrement, les travailleurs sont souvent - à tort - considérés comme des indépendants, excluant la possibilité de bénéficier d'avantages sociaux attachés au statut d'employé. En plus, plus de la moitié de ces personnes « *gagnent moins que le salaire minimum horaire net du pays où elles travaillent* ». ²
6. En outre, l'organisation par le biais d'algorithmes crée et/ou accentue des discriminations. Finalement, les plateformes soumettent les travailleurs à une surveillance numérique accrue.³
7. Le législateur européen, bien conscient de ces problématiques, développe actuellement un cadre juridique pour protéger ces travailleurs.⁴ Les autorités de contrôle jouent un rôle clé dans l'examen des pratiques des plateformes et dans le respect des droits de la personne concernée. Les autorités italiennes et

¹<https://www.consilium.europa.eu/fr/infographics/digital-platform-workers/>, consulté le 20.10.2026.

²<https://www.consilium.europa.eu/fr/infographics/digital-platform-workers/> consulté le 20.10.2026.

³Garante per la protezione dei dati personali, décision 10074601, du 13.11.2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>.

⁴<https://www.consilium.europa.eu/fr/infographics/digital-platform-workers/>, consulté le 20.10.2026.

néerlandaises ont par exemple récemment infligé des amendes à Glovo et Uber pour prise de décision automatisée illégale.⁵

3. LES FAITS DE L'AFFAIRE

3.1. La défenderesse

8. Scale AI est une société basée à San Francisco, aux États-Unis, qui, entre autres, est responsable du traitement pour Outlier, une plateforme d'annotation de données (ci-après la « Plateforme »).⁶
9. Via la Plateforme, la défenderesse organise le travail de centaines de milliers d'individus qui annotent les données et entraînent les IA pour des clients comme Meta, OpenAI, ou X.ai.⁷
10. Le travail est en général effectué selon le schéma suivant. Un client envoie des données à la défenderesse qui assigne (par le biais d'algorithmes) à un individu une tâche en lien avec ces données, par exemple les trier ou les étiqueter (« labeling ») selon certains critères, ou répondre à des prompts pour améliorer des LLM. La Plateforme examine ensuite les erreurs et assigne à un (autre) individu, la tâche de corriger et confirmer la qualité du travail fourni.

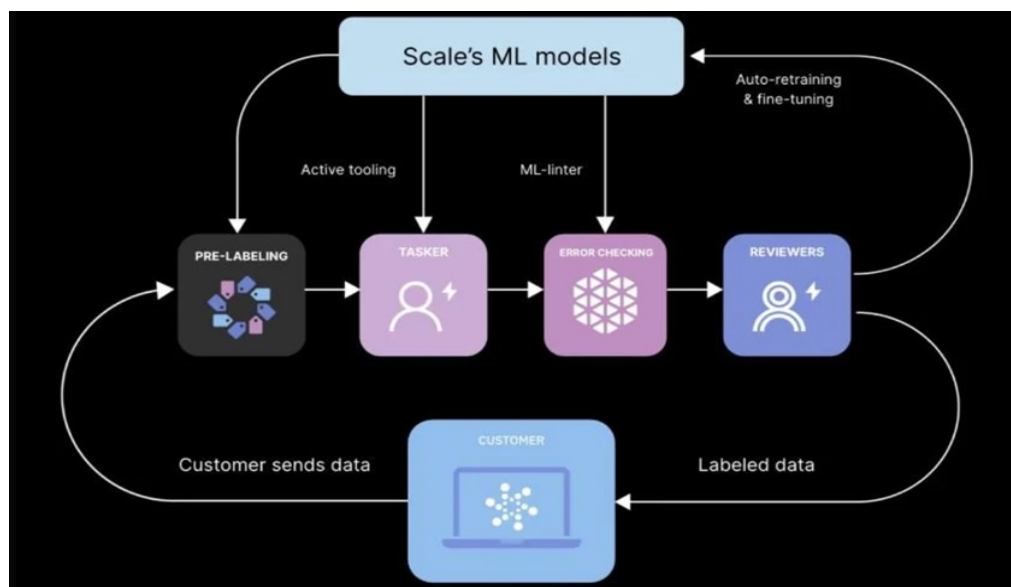


Figure 1: Schema de Scale AI (source: <http://www.leadrpro.com/blog/what-is-scale-ai-a-comprehensive-overview>)

⁵Autorité italienne de protection des données, décision n° 10074601, du 13 novembre 2024, Autorité néerlandaise de protection des données, <https://autoriteitpersoonsgegevens.nl/actueel/uber-krijgt-boete-van-bijna-825-miljoen-euro-voor-geautomatiseerd-blokkeren-van-chauffeurs>, consultée le 20.10.2026.

⁶<https://outlier.ai/legal/privacy-policy>, consulté le 20.10.2026.

⁷<https://www.inc.com/sam-blum/leaked-scale-ai-database-offers-new-details-into-projects-for-meta-google-and-x-ai/91176016>, consulté le 03.06.2026.

11. Les travailleurs, sont engagés sous le statut d'indépendant et non de salarié. Ils reçoivent une notification dès qu'une tâche leur est assignée et disposent alors d'une durée limitée pour la compléter, après quoi le taux horaire diminue (sur les conditions de travail au sein de la Plateforme, voir **l'annexe 3**).
12. Une tâche peut, par exemple, consister à comparer plusieurs réponses qu'un LLM pourrait générer en réponse à la requête d'un utilisateur. Elle peut également consister à corriger les réponses fournies par un LLM dans des domaines d'expertise spécifiques, tels que le codage, la physique ou les mathématiques.
13. La lecture de la politique de confidentialité⁸ de la défenderesse montre qu'elle traite de nombreuses données de ses travailleurs, dont une catégorie de données qu'elle collecte automatiquement (les « Données collectées Automatiquement »). Cette catégorie inclut l'identifiant unique de l'appareil utilisé, l'adresse IP, des informations collectées via des cookies ou pixels (non identifiés dans le document) ou encore le site consulté avant la Plateforme. La défenderesse traite ces données pour différentes finalités dont son « *intérêt légitime à opérer la plateforme* » (**annexe 4**).
14. La défenderesse indique également traiter les Données collectées Automatiquement pour son intérêt légitime à développer ses services et produits mais également à rechercher et tester des améliorations pour les services de ses clients, c'est à dire pour l'entraînement de leurs IA.

3.2. Le plaignant

15. Le [REDACTED], le plaignant a créé un compte sur la Plateforme. Pour ce faire, il a fait l'objet d'une vérification d'identité (voy. Section 3.3). Il a complété une cinquantaine de tâches pendant le mois d'avril 2025.
16. Celles-ci consistaient à comparer des modèles d'IA conversationnelle en donnant des notes à différentes réponses fournies par le LLM à un certain 'prompt'.
17. Après avril 2025, le plaignant n'a plus reçu de tâches et a continué de se connecter à la Plateforme à intervalles réguliers, dans l'attente de se voir attribuer de nouvelles tâches ou pour utiliser Playground AI, un service permettant aux travailleurs d'interagir avec divers modèles d'IA conversationnelle (Grok, Gemini, etc.).

⁸<https://outlier.ai/legal/privacy-policy>, consulté le 30.04.2026.

3.3. Traitement des données biométriques

18. Comme indiqué ci-dessus, pour créer son compte, le plaignant a dû vérifier son identité via un service tiers fourni par un sous-traitant : Persona.⁹¹⁰ Il lui a été demandé de téléverser une pièce d'identité, puis d'activer la caméra de son téléphone ou de son ordinateur pour enregistrer une vidéo de lui-même. La vérification a ensuite eu lieu à intervalles irréguliers (**annexe 5**).

19. La politique de vie privée de la Plateforme confirme l'expérience du plaignant : la vérification d'identité prend la forme d'un « selfie » photo ou vidéo ou d'un enregistrement vocal, accompagnée d'une analyse de la pièce d'identité. La Plateforme précise également que le traitement de ces données vise à *contribuer à préserver l'intégrité des Services et à lutter contre la fraude* en vérifiant les « compétences » et générant des informations sur le visage.

« (...) lorsque vous vous inscrivez pour utiliser les Services, puis à intervalles réguliers par la suite, nous pouvons collecter, stocker et analyser des images ainsi que des enregistrements vidéo ou audio vous représentant — y compris des selfies et des images de votre pièce d'identité officielle — et utiliser ces images et enregistrements pour vérifier vos qualifications ou générer des informations et des mesures concernant votre visage (« Données de vérification »), qui peuvent être considérées comme des données « biométriques » ou « sensibles » en vertu des lois de certaines juridictions »¹¹ (traduction libre, nous soulignons).

20. Persona traite les données qui lui sont transmises conformément à sa politique de confidentialité, à laquelle la défenderesse renvoie. Ce document décrit notamment le traitement effectué par Persona dans le cadre de la fourniture de son service. Il convient notamment de noter que Persona se réserve le droit de collecter des données auprès d'un nombre illimité de « tiers » non définis et ne fournit que des catégories générales d'informations collectées via une liste ouverte, qui « comprend » les adresses IP, les informations sur les appareils, les données de géolocalisation, les identifiants uniques, les données d'adresse, les données de crédit à la consommation et d'autres données :

« Nous pouvons également collecter les informations suivantes auprès de vous, notre client, ou auprès de tiers afin de déterminer et de mettre en œuvre la méthode de vérification d'identité adaptée à votre juridiction et de garantir le respect des lois et règlements applicables :

*- **des informations sur l'appareil**, notamment l'adresse IP, le type d'appareil, le système d'exploitation de votre appareil, le navigateur, les cookies et les identifiants de l'appareil, ainsi que d'autres logiciels, y compris leur type, leur version, leur langue, leurs paramètres et leur configuration ;*

⁹<https://withpersona.com/legal/idv-privacy-policy?ajs=e34c9eb2-fc5d-42ba-881a-3e4a542d2e57#8-contact-us>, consulté le 20.10.2026.

¹⁰<https://outlier.ai/legal/privacy-policy>, consulté le 20.10.2026.

¹¹<https://outlier.ai/legal/privacy-policy>, consulté le 20.10.2026.

- (...) **des données accessibles au public**, y compris celles issues de registres publics et des réseaux sociaux ;
- (...) **Données supplémentaires de vérification de l'âge** : nous pouvons vérifier vos données à caractère personnel à des fins de vérification de l'âge selon une finalité par le biais de notre réseau de sources de données tierces de confiance, notamment : des sources accessibles au public (telles que les bases de données gouvernementales ouvertes), les registres d'identité nationaux et gouvernementaux, les agences d'évaluation du crédit à la consommation, les entreprises de services publics, les opérateurs de réseaux mobiles et les bases de données d'adresses postales. Les types de « données supplémentaires de vérification de l'âge » que nous obtenons de ces sources varient en fonction des contrôles de vérification disponibles dans le pays concerné. »¹² (traduction libre, nous soulignons)

21. Persona fait actuellement appel à une quinzaine de sous-traitants, dont OpenAI, Groqcloud et Anthropic, pour diverses tâches d'extraction et analyse de données.¹³ Le traitement des données s'effectue via des infrastructure basées aux États-Unis, notamment Amazon Web Services et Google Cloud.¹⁴
22. Des pratiques de sécurité douteuses de la part de Persona ont également été signalées. Par exemple, en octobre 2025, environ 70 000 photos de pièces d'identité officielles stockées chez Persona ont été dérobées par des hackers. En février 2026, le code source de Persona a été trouvé en libre accès.¹⁵ Ce code a notamment montré que (i) pour chaque « vérification d'identité », Persona peut effectuer 269 contrôles distincts dont des comparaisons entre les données fournies et des bases de données ; et (ii) Persona filtre les « médias défavorables » selon 14 catégories (dont le terrorisme et l'espionnage), et attribue des scores de risque et de « similarité ».¹⁶
23. Persona a confirmé ces failles de sécurité.¹⁷ Ces pratiques ont d'ailleurs conduit l'un de ses principaux clients, la plateforme Discord, à résilier son contrat avec Persona concernant la vérification de l'âge de ses utilisateurs.¹⁸

¹²<https://withpersona.com/legal/privacy-policy>, consulté le 20.10.2026.

¹³<https://withpersona.com/legal/subprocessors>, consulté le 20.10.2026.

¹⁴<https://withpersona.com/legal/subprocessors>, consulté le 20.10.2026.

¹⁵<https://vmfunc.re/blog/persona> , https://www.franceinfo.fr/internet/reseaux-sociaux/la-plateforme-discord-repousse-la-verification-d-age-pour-la-fin-2026-apres-des-critiques-sur-la-securite-des-donnees_7829012.html, consulté le 20.10.2026.

¹⁶<https://www.malwarebytes.com/blog/news/2026/02/age-verification-vendor-persona-left-frontend-exposed> et <https://vmfunc.re/blog/persona> https://www.franceinfo.fr/internet/reseaux-sociaux/la-plateforme-discord-repousse-la-verification-d-age-pour-la-fin-2026-apres-des-critiques-sur-la-securite-des-donnees_7829012.html, consultés le 20.10.2026.

¹⁷<https://withpersona.com/blog/post-incident-review-source-map-exposure-non-production-subdomain>, consulté le 20.10.2026.

¹⁸https://www.franceinfo.fr/internet/reseaux-sociaux/la-plateforme-discord-repousse-la-verification-d-age-pour-la-fin-2026-apres-des-critiques-sur-la-securite-des-donnees_7829012.html, consulté le 20.10.2026.

24. La politique de vie privée de Persona a été mise à jour le 9 avril 2026. Sa version précédente, en vigueur depuis l'inscription du plaignant,¹⁹, prévoyait la possibilité de réaliser le traitement de documents d'identité à des fins d'« entraînement du service » via ses systèmes d'IA (voir capture d'écran ci-dessous).²⁰

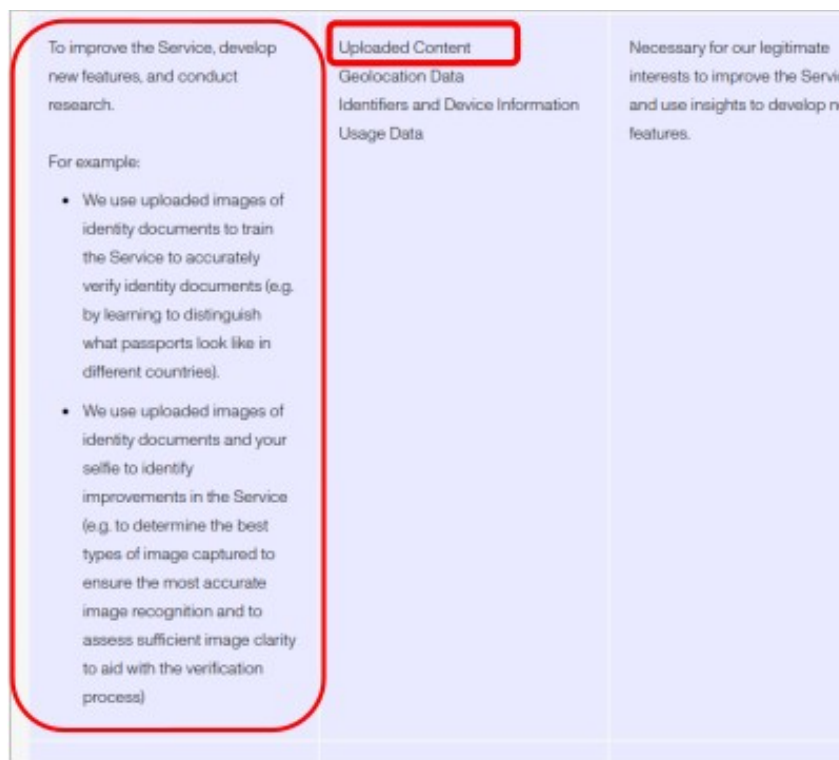


Figure 2: Politique de confidentialité avant le 9 avril 2026

3.4. Analyse du trafic

25. Le [REDACTED] le plaignant a capturé le trafic sur la Plateforme sous la forme de deux fichiers HAR²¹ durant [REDACTED] minutes, alors qu'il naviguait sur la Plateforme (**annexes 6 et 7**). Il a réalisé cette capture en utilisant la méthodologie décrite en annexe (**annexe 8**).

26. Les fichiers HAR montrent que la Plateforme contient des traceurs²² placés par les tiers suivants: Fullstory, Sprig, LinkedIn, TikTok, Facebook, Posthog, Segment,

¹⁹Voir, par exemple, la version datée du 12 janvier 2025 :

<https://web.archive.org/web/20250112151512/https://withpersona.com/legal/idv-privacy-policy>, consulté le 20.10.2026.

²⁰ La politique de vie privée de Persona est disponible à l'adresse <https://withpersona.com/legal/idv-privacy-policy>, consulté le 20.10.2026. La version mise à jour le 9 avril 2026 est disponible ici : <https://web.archive.org/web/20260422094923/https://withpersona.com/legal/idv-privacy-policy>

La version mise à jour le 8 mai 2025, qui comprend une déclaration concernant l'utilisation par le service des documents téléchargés par les Utilisateurs à des fins de formation, est disponible ici : <https://web.archive.org/web/20260326065823/https://withpersona.com/legal/idv-privacy-policy>

²¹ Un fichier HAR (abréviation de *HTTP Archive*) est un journal complet des interactions entre un navigateur et des serveurs web au cours d'une session de navigation.

Quora, Forethought, Sentry, Snapchat, Run.app, Twitter Analytics, Google Analytics, Recruitics, Withpersona, Amplitude et Featureassets.

27. La figure 3 présente le nombre de requêtes identifiées pour certains de ces tiers dans l'annexe 7.²³ Des explications plus détaillées concernant certains exemples de traceurs sont fournies ci-après.

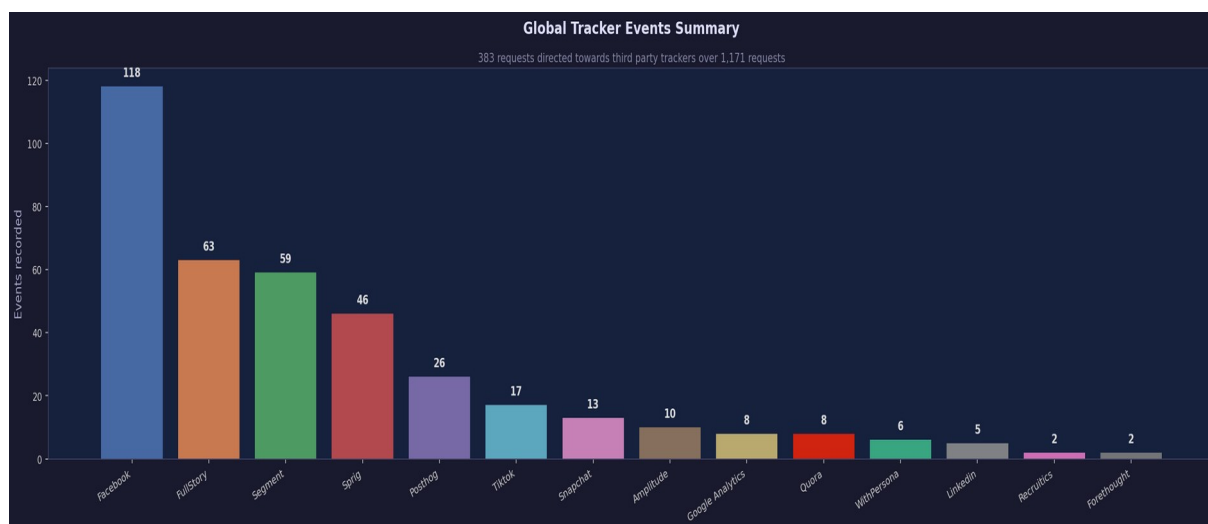


Figure 3: Traceurs trouvés dans les annexes 6 et 7

Exemple 1 : traceurs « réseaux sociaux »

28. Les fichiers HAR révèlent la présence de traceurs provenant de Facebook, TikTok, Snapchat et LinkedIn. Le traceur Facebook, par exemple, envoie un nombre significatif de requêtes. Ces requêtes attribuent notamment un identifiant unique (« workerTeamId ») au plaignant (ici, [REDACTED]), un identifiant au projet (« projectId »), identifient si le plaignant s'est vu attribuer une tâche (dans ce cas, non) et expliquent pourquoi il n'a pas de tâches — en l'occurrence, parce qu'aucune tâche ne correspond à son expertise (« [REDACTED] »). Ce tracker comprend également des identifiants (tels que « [REDACTED] ») qui permettent à Meta d'associer les visites de sites web aux navigateurs des utilisateurs, ce qui est généralement utilisé à des fins de publicité ciblée.²⁴

²² Un traceur est un outil — souvent invisible — qui recueille des informations sur le comportement en ligne d'une personne. Il peut enregistrer les sites web visités, les pages consultées, le temps passé sur un contenu, la localisation approximative de l'utilisateur, le type d'appareil utilisé, etc. « Un pixel de suivi est une méthode de suivi alternative aux cookies, traditionnellement mise en œuvre sous la forme d'une image de 1 pixel sur 1 pixel intégrée au site web mais invisible pour l'utilisateur. Le chargement de cette image, dont le nom contient un identifiant d'utilisateur, informe le serveur qui l'héberge que l'utilisateur suivi a visité une page ou lu un e-mail. » Voir <https://www.cnil.fr/fr/definition/tracking-pixelweb-beacon-ou-pixel-espion>, consulté le 20.10.2026.

²³ Une requête est une demande envoyée par un programme ou un appareil à un autre, dans l'attente d'une réponse en retour.

²⁴ <https://pantosource.com/blog/meta-ads-data-quality?>, consulté le 20.10.2026

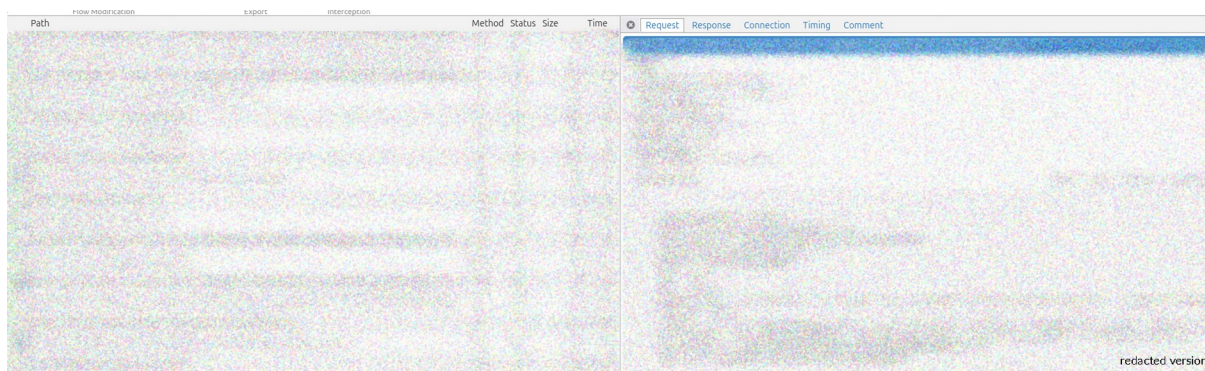


Figure 4: Traceur Facebook (extrait annexe 6)

Exemple 2 : le traceur Forethought

29. Forethought Technologies Inc. est une entreprise américaine qui propose une plateforme d'IA dédiée au support client.²⁵ Le traceur Forethought détecté dans les fichiers HAR comprend, entre autres, les éléments suivants : identifiant unique (« data-ft-corp-user-id »), nom, prénom et adresse e-mail du plaignant (**annexe 6**).

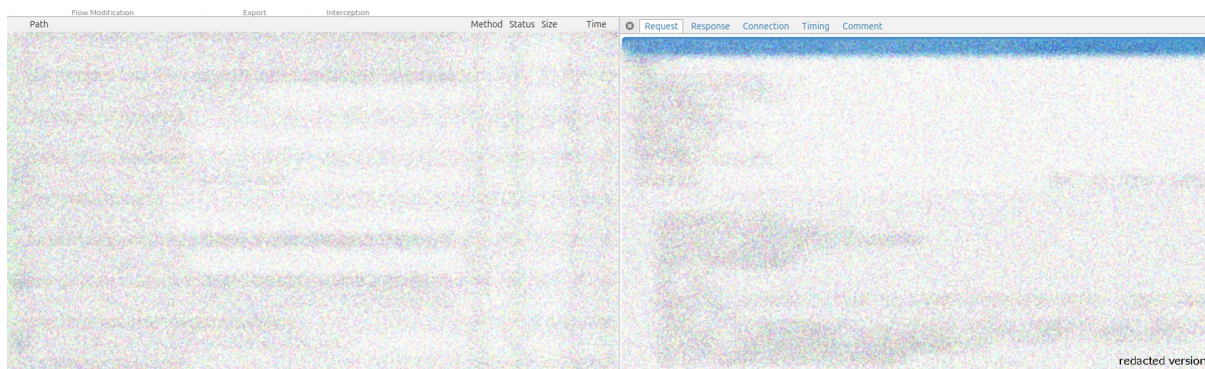


Figure 5 : Traceur Forethought — extrait de l'annexe 6

Autres exemples

30. Fullstory propose un outil de rejeu de session qui enregistre les mouvements de souris, les clics, les frappes au clavier, etc.²⁶ Dans ce cas, le tracker Fullstory envoie une requête toutes les quelques secondes. Il enregistre des événements particuliers : statut des tâches (nombre de tâches disponibles et accomplies) ainsi que les tâches encore disponibles (voir annexes 6 et 7).

31. En particulier, les champs « SetNodeAttribute » et « SetInputValue » indiquent ce qui est saisi dans les champs de formulaire. « PointerEvent / NetworkReq » indiquent les mouvements du curseur (c'est-à-dire de la souris) et les requêtes

²⁵ <https://forethought.ai/>, consulté le 20.10.2026.

²⁶ Voy. la présentation vidéo de Full Story sur son travail : <https://www.youtube.com/watch?v=Q18TO1lZVz8>, consultée le 20.10.2026.

réseau. « input_fields_active » et « input_max_chars » suivent les champs de saisie, et « is_mobile » indique si l'utilisateur utilise un appareil mobile.

32. Un autre traceur est déployé par Sprig²⁷, qui fournit des outils d'enquête internes qu'un employeur peut faire remplir à ses salariés. Dans ce cas précis, le plaignant ne répondait pas à une enquête au moment de l'analyse, mais l'outil de suivi recueille, entre autres, son nom, prénom, adresse e-mail et numéro de téléphone.

3.6. La demande d'accès

33. Le 02.02.2026, le plaignant a envoyé une demande d'accès aux adresses privacy@outlier.ai et outlier@lionheartssquared.eu, comme précisé dans la politique de confidentialité de la Plateforme (**annexe 9**). La demande avait en particulier pour objet de prendre connaissance de l'existence de prise de décision automatique à son sujet.
34. La défenderesse n'a jusqu'à présent pas fait suite à cette demande.
35. Le 12.05.2026, le plaignant a également contacté Persona pour demander accès à ses données personnelles. Hormis un accusé de réception, cette demande est également restée sans réponse (**annexes 10 et 11**).

4. AUTORITÉ COMPÉTENTE

36. Le plaignant réside et travaille en France, et la défenderesse est établie aux États-Unis, sans établissement principal dans l'Union. La CNIL est donc compétente pour traiter cette réclamation conformément à l'article 77 du RGPD.

5. EN DROIT

5.1. Violations

37. Les pratiques examinées peuvent être classées en trois catégories : (1) le placement de traceurs ; (2) le traitement des données biométriques ; et (3) la demande d'accès. Elles constituent respectivement des violations de

- (1.a) l'Article 5(1)(c) RGPD en traitant les données du plaignant et plaçant des traceurs en violation du principe de minimisation;
- (1.b) l'article 5(3) de la directive 2002/58/CE concernant la vie privée et les communications électroniques (ePrivacy), transposée en France par l'article 82

²⁷<https://sprig.com/>, consulté le 20.10.2026.

de la loi informatique et libertés, en plaçant des traceurs sur le terminal du plaignant sans son consentement ;

(2) Articles 5(1)(c) *juncto* 25(1) et 28(1) RGPD en traitant les données biométriques du plaignant en violation du principe de minimisation, du choix du sous-traitant adéquat et de la protection des données par défaut;

(3) Articles 15 et 12(3) RGPD en ne répondant pas à la demande d'accès du plaignant.

(1.a) Violation de l'article 5(1)(c) RGPD

38. Le principe de minimisation est une application du principe de proportionnalité qui impose qu'une ingérence dans un droit fondamental soit proportionnée.²⁸ En particulier, l'Article 5(1)(c) RGPD requiert que les données traitées soient adéquates, pertinentes et limitées à ce qui est strictement nécessaire pour les finalités poursuivies.

39. En l'espèce, comme décrit ci-dessus (§13), la défenderesse traite les Données collectées Automatiquement telles que l'adresse IP, le site consulté par le plaignant avant la Plateforme, des informations qui identifient uniquement l'appareil et les traceurs examinés *supra* (point 3.4).

40. Les finalités déclarées du traitement de ces données sont les suivantes :

- fournir, opérer et administrer la Plateforme ;
- la personnalisation du service ;
- l'amélioration des produits et services de la défenderesse ; et
- l'amélioration des produits et services des clients de la défenderesse.²⁹

41. Un autre document, la politique « cookies » de la Plateforme fait également référence aux finalités de profilage et de publicité ciblée.³⁰

42. Il est difficile d'envisager en quoi le traitement de toutes les données collectées automatiquement, y compris via les traceurs décrits au point 3.4, serait strictement nécessaire à la poursuite des finalités citées. Par exemple, connaître le site consulté avant la Plateforme n'est manifestement nécessaire à la poursuite d'aucune finalité.

²⁸ CJUE, *NTH Haustechnik GmbH*, C-484/24, 18 juin 2026, §95.

²⁹ <https://outlier.ai/legal/privacy-policy>, consulté le 20.10.2026.

³⁰ <https://outlier.ai/legal/cookies-policy>, consulté le 20.10.2026.

43. Concernant l'amélioration des produits et services des clients de la défenderesse, ce qui inclut certainement l'entraînement de leurs IA, sans même évoquer les sérieux doutes sur la légalité de cette finalité, il apparaît disproportionné que les données du plaignant, en particulier celles traitées par le biais des traceurs, l'adresse IP, ou le site consulté avant la Plateforme soient traitées pour cette finalité.
44. L'analyse du trafic a également montré que de nombreux traceurs sont placés par des réseaux sociaux, sociétés d'analytics et fournisseurs de services divers. Comme décrit *supra*, des données telles que les coordonnées du plaignant, son activité sur la plateforme, ses mouvements de souris ou encore des identifiants uniques sont ainsi traitées. À nouveau, il est difficile d'imaginer en quoi un traitement aussi systématique et constant, au profit de tellement de destinataires serait strictement nécessaire à la poursuite des finalités citées.
45. Concernant les réseaux sociaux, en particulier, les finalités poursuivies par la Plateforme sont complètement distinctes de finalités de réseaux sociaux. Il est donc d'autant plus difficile d'établir l'utilité du traçage, et encore moins sa nécessité.
46. Il convient également de noter que toutes ces finalités sont présentées comme étant poursuivies dans les intérêts légitimes de la Plateforme. Conformément à l'article 6(1)(f) RGPD, tel qu'interprété par la CJUE et l'EDPB, cette base juridique requiert, en particulier, que les données soient traitées conformément au principe de minimisation pour être valable.³¹ Une violation du principe de minimisation emporte donc une invalidité de la base légale de l'intérêt légitime.
47. Pour se conformer au principe de minimisation, la défenderesse aurait pu, par exemple, pour la finalité d'améliorer ses produits et services, traiter uniquement certaines données relatives aux appareils, telles que le navigateur utilisé, la langue et le type d'appareil utilisé (mobile ou ordinateur), ou traiter certaines données uniquement lors d'événements déclencheurs spécifiques comme des « bugs ». En ce qui concerne les traceurs, la défenderesse aurait également dû supprimer un certain nombre d'entre eux et/ou limiter le traitement des données pouvant être effectuées par leur intermédiaire. En particulier, s'agissant des outils de rejeu de session, la défenderesse aurait pu, comme le recommande la CNIL dans son projet de recommandations sur les outils de relecture de session,³² n'utiliser l'outil

³¹ CJUE, C-252/21, *Meta c. Bundeskartellamt*, par. 109 ; C-708/18, *Asociația de Proprietari bloc M5A-ScaraA*, par. 48 ; C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, par. 51 à 52 ; EDPB, Lignes directrices n° 1/2024 relatives au traitement des données à caractère personnel fondé sur l'article 6, paragraphe 1, point f), du RGPD, 8 octobre 2024, point 29.

³² https://www.cnil.fr/sites/default/files/2026-02/projet_de_recommandation_rejeu_session.pdf, consulté le 20.10.2026.

qu'occasionnellement et de manière aléatoire, mettre en œuvre une technique de masquage ou de hachage, ou éviter de collecter des identifiants uniques.

48. L'autorité italienne a eu l'occasion d'examiner le placement de certains traceurs à finalités analytiques sur le terminal de travailleurs. Ces traceurs, tout comme en l'espèce, permettaient le traitement de l'identifiant des travailleurs, leur adresse IP, données relatives à l'appareil et email et numéro de téléphone. L'autorité a qualifié le traitement aussi massif et le partage des données avec des tiers de surveillance, en violation du principe de minimisation.³³

49. Il résulte ainsi de ce qui précède que les données du plaignant ont été traitées en violation du principe de minimisation de l'Article 5(1)(c) RGPD.

(1.b) Violation de l'article 5(3) de la directive ePrivacy et de l'article 82 de la loi informatique et libertés

50. Le placement de pixels et traceurs constitue un stockage sur le terminal de l'utilisateur et est donc également régi par l'article 5(3), de la directive ePrivacy.³⁴

51. L'article 82 de la loi informatique et libertés, transpose l'article 5(3), de ladite directive et dispose que

« Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :

1° De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;

2° Des moyens dont il dispose pour s'y opposer. Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son consentement qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.

Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

1° Soit, a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;

2° Soit, est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur. »

³³Garante per la protezione dei dati personali, décision 10074601, du 13.11.2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, section 4.11.

³⁴EDPB, Guidelines 2023/02 on Technical Scope of Art. 5(3) of ePrivacy Directive, §50.

52. En l'espèce, l'analyse de trafic ainsi que la lecture de la politique de confidentialité (voy. *supra*, section 3.1) ont démontré que la défenderesse a placé des traceurs et pixels sur le terminal du plaignant.

53. La défenderesse se fonde sur son intérêt légitime pour placer ces traceurs, ce qui constitue une violation de l'article 82 précité qui exige un consentement de la part de la personne concernée.

(2) Violation des Articles 5(1)(c) *juncto* 25(1) et 28(1) RGPD

54. L'Article 25(1) RGPD impose aux responsables de traitement de prendre les mesures techniques et organisationnelles adéquates pour assurer que les principes comme la minimisation et la légalité soient respectés au bénéfice des personnes concernées.

55. L'EDPB précise que les responsables de traitement ne doivent pas choisir de sous-traitant qui ne leur permettent pas de se conformer à leurs obligations, puisqu'ils sont responsables du respect de l'Article 25 RGPD.³⁵ En d'autres termes, les mesures adéquates incluent le choix d'un sous-traitant adéquat.³⁶

56. Dans le même sens, l'Article 28(1) RGPD impose également aux responsables de traitement de choisir des sous-traitants capables de garantir le respect du RGPD.

57. Ces mesures sont particulièrement pertinentes lorsqu'il est question de traitement de données sensibles en vertu de l'Article 9 RGPD, comme les données biométriques. L'EDPB précise à cet égard que le traitement de ces données constitue « *en soi* » une atteinte grave à la vie privée.³⁷ Les mesures peuvent consister en une pseudonymisation ou à obliger les sous-traitants à implémenter certaines pratiques de minimisation.³⁸

58. L'autorité de contrôle italienne a jugé, dans une affaire où une entreprise exigeait de ses travailleurs de plateforme qu'ils s'identifient par le biais d'une vérification

³⁵https://www.edpb.europa.eu/sites/default/files/files/file1_edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, consulté le 20.10.2026, §96.

³⁶Dans le même sens, Garante per la protezione dei dati personali, décision 10074601, du 13.11.2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, section 4.11.

³⁷Lignes directrices 05/2022 sur l'utilisation de la technologie de reconnaissance faciale dans le domaine répressif, 26 avril 2023, §36.

³⁸https://www.edpb.europa.eu/sites/default/files/files/file1_edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, consulté le 20.10.2026, §9.

biométrique, que le traitement de ces données n'était pas indispensable à la fourniture du service en question.³⁹

59. Il est incontestable que la défenderesse effectue le traitement des données biométriques du demandeur aux fins de vérification d'identité et d'âge. La présente section démontre (i) que le traitement de données biométriques en soi n'est pas strictement nécessaire, en violation de l'Article 5(1)(c) RGPD et (ii) que même s'il l'était, le traitement tel que délégué à Persona a toutefois été exécuté en violation des Articles 5(1)(c) *juncto* 25(1) et 28(1) RGPD.

(i) Le traitement des données biométriques n'est pas nécessaire

60. Le traitement de données biométriques est ici effectué « *afin de contribuer à préserver l'intégrité des Services et de lutter contre la fraude* ». ⁴⁰ Les termes vagues laissent supposer qu'il s'agit ici de s'assurer que c'est bien le travailleur recruté qui effectue les tâches. Dans le cas italien précité, le responsable de traitement poursuivait une finalité similaire et concédait durant la procédure que la vérification biométrique ne constitue pas *per se* une mesure suffisante pour prévenir le phénomène mais plutôt un moyen de dissuasion. L'autorité italienne avait donc conclu que la vérification biométrique n'était pas strictement nécessaire. ⁴¹ Cette considération est valable *mutatis mutandis* en l'espèce.

61. En réalité, pour poursuivre la finalité annoncée, il existe d'autres moyens moins intrusifs d'authentifier les travailleurs. L'on pense par exemple à l'identification à deux facteurs (2FA) ou à une clé physique à insérer pour se connecter.

(ii) Même si l'autorité considérait le traitement comme nécessaire, il viole les articles 5(1)(c), 25(1) et 28(1)

62. Sans réponse à sa demande d'accès, le plaignant ne peut que se fonder sur la politique de confidentialité de Persona qui, comme décrit ci-dessus, indique traiter des données relatives à l'appareil utilisé, l'adresse IP et autres données et également comparer les données qu'elle reçoit avec des données issues d'autres bases de données. Cela correspond à une technique d'identification dite *one-to-many* qui consiste à comparer un visage avec d'autres visages, présents dans une base de donnée. L'on oppose la technique *one-to-many* à la technique de vérification *one-to-one* qui consisterait ici à comparer un visage avec un document d'identité.

³⁹ Garante per la protezione dei dati personali, décision n° 10074601, du 13 novembre 2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, section 4.7.

⁴⁰ <https://outlier.ai/legal/privacy-policy>, consulté le 20.10.2026.

⁴¹ Garante per la protezione dei dati personali, décision 10074601, du 13.11.2024, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10074601>, section 4.7.

63. La directive (UE) 2024/2831 du Parlement européen et du Conseil du 23 octobre 2024 relative à l'amélioration des conditions de travail dans le cadre du travail via une plateforme, bien que pas encore transposée, peut être utile pour mener l'examen de la légalité de ce type de vérifications. Son considérant 41 indique expressément que si le traitement de donnée biométrique doit avoir lieu, c'est la vérification par la technique *one-to-one* qui doit être préconisée.
64. En l'espèce, le traitement des données susmentionnées est manifestement excessif par rapport à la finalité poursuivie, soit la vérification de l'identité.
65. Pour être effectuée dans le respect du principe de minimisation, la vérification devrait être effectuée par la technique *one-to-one* et Persona ne devrait pas pouvoir collecter d'autres données que celles strictement nécessaires. C'est bien à la défenderesse qu'il revient de choisir un prestataire adéquat pour cette vérification et de ne lui permettre de collecter que certaines données.
66. Noyb a par ailleurs également connaissance d'une autre personne concernée qui a enregistré le trafic lors de la vérification de son identité avec Persona. Cela a montré que Persona effectue le traitement de données relatives à l'appareil utilisé, à l'adresse IP et à d'autres données.
67. En imposant au plaignant un traitement de ses données biométriques en violation du principe de minimisation, la défenderesse a non seulement violé ce principe mais également son obligation de prendre les mesures techniques et organisationnelles adéquates, qui incluent le choix d'un fournisseur de service, sous-traitant, adéquat. En conclusion, la défenderesse a violé les Articles 5(1)(c), 25(1) et 28(1) RGPD.

(3) Violation des articles 15 et 12(3) RGPD

68. L'Article 15 RGPD impose aux responsables de traitement de faire droit aux demandes d'accès des personnes concernées. L'Article 12(3) RGPD impose de répondre dès que possible et au plus tard dans le mois de la demande.
69. En l'espèce, le plaignant soupçonnait faire l'objet de prise de décision automatisée et avait expressément demandé à la défenderesse de l'en informer (**annexe 9**). Cette demande est restée lettre morte. En ne faisant pas suite à la demande d'accès du plaignant, la défenderesse a violé l'Article 15 RGPD et forcément l'Article 12(3) RGPD.

6. DEMANDES

6.1. Décision déclaratoire

70. Le plaignant demande à l'autorité de constater les violations suivantes établies dans le chef de la défenderesse :

- la violation de l'Article 5(1)(c) RGPD en traitant des données du plaignant qui n'étaient pas nécessaires aux finalités poursuivies ;
- la violation de l'Article 82 de la loi informatique et libertés en plaçant les traceurs et pixels sans consentement du plaignant ;
- la violation des Articles 5(1)(c), 25(1) et 28(1) RGPD par la défenderesse en traitant les données biométriques et faisant appel à un sous-traitant ne prenait pas en compte (entre autres) le principe de minimisation ;
- la violation des Articles 12(3) et 15 en ne répondant pas à la demande d'accès

6.2. Accès

71. Le plaignant demande à l'autorité d'ordonner à la défenderesse de faire droit à sa demande d'accès.

6.3. Enquête

72. Le plaignant demande à l'autorité d'enquêter sur les violations exposées dans la plainte et d'étendre son enquête aux pratiques de la défenderesse en matière de prise de décision automatisée.

6.4. Suggestion d'imposer une amende

73. Le plaignant suggère que l'autorité de contrôle inflige une amende administrative au responsable du traitement, conformément aux Articles 58(2)(i), et 83(5)(a) et (b), du RGPD pour les infractions relevées.

6.5. Suggestion de sanction publique

74. Le plaignant suggère que l'identité de la défenderesse soit rendue publique dans la décision.

7. CONTACT

75. Les communications entre *noyb* et l'autorité de contrôle dans le cadre de la présente procédure peuvent être envoyées par e-mail à l'adresse [REDACTED], en mentionnant le numéro de dossier C109-01, ou par téléphone au [REDACTED]