RÉCLAMATION AUPRÈS DE LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

–

CLEARVIEW AI, INC.

I. Introduction et objectif de cette réclamation

1. Par la présente réclamation, Privacy International (ci-après « **PI** ») fournit à la Commission Nationale de l'Informatique et des Libertés (ci-après « **CNIL** ») des éléments de preuve et d'analyse afin de contribuer à son enquête en cours sur la conformité de la société Clearview AI, Inc. (ci-après « **Clearview** ») avec la législation sur la protection des données, en particulier le Règlement général sur la protection des données ((UE) 2016/679) (ci-après « **RGPD** ») et la directive n° 2016/680 dite directive *Police-Justice* (ci-après « **directive Police-Justice** ») transposée en droit français par le titre III de la loi n°78-17 du 6 janvier 1978 dite *Loi Informatique et Libertés* (ci-après « **LIL** »).

2. Les pratiques de Clearview en matière de données et les utilisations de la plateforme que l'entreprise a développée sont à l'origine de violations substantielles et continues du RGPD et de la LIL. Au terme de développements introductifs, la présente réclamation s'articulera autour des deux principales étapes de l'impact de l'activité de Clearview sur les personnes concernées en France : (1) le traitement initial de données à caractère personnel par Clearview à-travers la collecte, le stockage et l'identification (section V), et (2) l'utilisation des services de Clearview par les forces de l'ordre (section VI).

II. Privacy International

3. PI est une organisation non gouvernementale à but non lucratif, basée à Londres, qui travaille dans le monde entier à l'intersection des nouvelles technologies et des droits humains. Fondée en 1990, PI entreprend des recherches, des procédures judiciaires et du plaidoyer pour construire un avenir où les technologies, les lois et les pratiques contiennent des protections modernes pour éviter l'exploitation des personnes et de leurs données. En tant que telle, PI a des objectifs statutaires d'intérêt public et est active dans le domaine de la protection des droits et libertés des personnes concernées. PI est donc éligible pour agir en vertu de l'article 37 paragraphe 4 point 1 de la LIL. Cette réclamation concerne les travaux en cours de PI sur l'exploitation des données par les entreprises, la surveillance des réseaux sociaux et la reconnaissance faciale.

III. Le responsable de traitement - Clearview AI, Inc.

4. Clearview AI, Inc. est une société basée aux Etats-Unis, fondée en 2017. Son unique produit est une plateforme de reconnaissance faciale permettant aux utilisateurs de faire correspondre des photos d'individus à des images de ces mêmes personnes trouvées en ligne. La plateforme de Clearview « comprend la plus grande base de données connue de plus de trois milliards d'images faciales provenant de sources accessibles en ligne exclusivement publiques, y compris des sites journalistiques, des sites contenant des photos d'identité judiciaire, des profils de réseaux sociaux accessibles au public, ainsi que d'autres sources accessibles librement. »[1]

5. En 2020, Clearview comptait environ 2 900 utilisateurs actifs. Bien que tous ses documents de marketing accessibles au public soient destinés aux forces de l'ordre, les clients de Clearview iraient des « départements de sécurité d'universités aux bureaux des procureurs généraux » et incluraient « un nombre étonnant d'entreprises privées dans des secteurs comme le divertissement (Madison Square Garden et Eventbrite), les jeux d'argent (Las Vegas Sands et Pechanga Resort Casino), le sport (la NBA), le fitness (Equinox) et même la crypto-monnaie (Coinbase) ».[2] Certaines sources ont également indiqué que des particuliers avaient utilisé la plateforme de Clearview « lors de rendez-vous et de fêtes – et pour espionner le public ».[3]

Description technique de la base de données d'images et du produit Clearview

6. D'après notre enquête et notre analyse de sources librement accessibles au public,[4] ainsi que notre propre expertise technique, nous estimons que la base de données d'images créée par Clearview pour sa plateforme de reconnaissance faciale est alimentée en quatre étapes :

    1) **Le dispositif automatisé de récupération d'images (le *scraper*)** – un outil automatisé recherche les pages web publiques et récupère toutes les images qu'il détecte comme contenant des visages humains. Avec ces images, le *scraper* collecte également les métadonnées qui y sont

[1] Vue d'ensemble (Clearview AI), https://clearview.ai/overview.
[2] BuzzFeed News, 'Clearview's Facial Recognition App Has Been Used by The Justice Department, ICE, Macy's, Walmart, And the NBA' (27 février 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.
[3] Kashmir Hill, 'Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich' (The New York Times, 5 mars 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html.
[4] Commissariat à la protection de la vie privée du Canada (CPVP), Rapport de conclusions d'enquête en vertu de la LPRPDE no 2021-001 (2 Février 2021), https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2021/lprpde-2021-001/ ; Clearview AI, 'Law Enforcement' (site Web de Clearview AI), https://clearview.ai/law-enforcement ; Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Letter to Clearview AI Inc. - Consultation prior to an order pursuant to Article 58(2)(g) RGPD (27 janvier 2021), https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF.

associées, telles que le titre de l'image ou de la page web, le code source et la géolocalisation.[5]

2) **Stockage des images et des métadonnées** – les images et les métadonnées collectées via la méthode de scraping sont stockées sur les serveurs de Clearview. Elles sont stockées indéfiniment, c'est-à-dire même après qu'une photographie ou une page web d'hébergement précédemment collectée a été supprimée ou que son contenu ait été rendu privé.

3) **Extraction des caractéristiques du visage par des réseaux neuronaux de traitement d'image** – pour chaque image collectée, chacun des visages contenus dans l'image est scanné et traité afin d'en extraire les caractéristiques qui l'identifient de manière unique. Les visages sont traduits en représentations numériques que nous appelons « vecteurs ». Ces vecteurs sont composés de 512 points de données qui représentent les différentes lignes uniques qui composent un visage. À ce stade, les visages sont convertis d'images reconnaissables par l'humain en identifiants numériques biométriques uniques lisibles par les machines.

4) **Stockage et indexation/hachage des caractéristiques du visage** – Clearview stocke ces vecteurs dans une base de données sur son serveur, où ils sont associés aux images et autres informations récupérées via son outil de *scraping*. Ces vecteurs sont ensuite hachés (le hachage consistant à transformer un vecteur par le biais d'une fonction mathématique en une valeur plus courte de longueur fixe ou en une clé qui représente le vecteur d'origine), pour remplir deux finalités connexes : l'indexation de la base de données et l'identification future des visages. Chaque visage de la base de données est associé à un vecteur distinct et à une valeur de hachage spécifique afin de permettre l'identification et la correspondance.

7. La cinquième et dernière étape du cycle de vie du produit Clearview est la **mise en correspondance**. Elle est effectuée lorsqu'un utilisateur de Clearview souhaite identifier un individu, et pour cela téléverse une image de cette personne et lance une recherche. Clearview analyse alors l'image et extrait un vecteur du visage de la personne recherchée, qui est ensuite haché et comparé à tous les vecteurs hachés précédemment stockés dans sa base de données. Enfin, l'outil Clearview extrait toutes les images correspondantes de sa base de données vectorielle et les présente à l'utilisateur sous forme de résultats de recherche, assortis de toutes les métadonnées associées, ce qui permet à l'utilisateur de prendre connaissance de la page d'origine des images correspondantes.

IV. <u>Contexte</u>

A. Les « révélations » Clearview et l'intérêt de différentes autorités de contrôle

[5] Clearview AI, Inc. Politique de confidentialité (version 1, dernière mise à jour le 29 janvier 2020), https://clearview.ai/privacy/privacy_policy. Voyez aussi Pièce n°2, réponse à la demande de droit d'accès de [redacted] à Clearview AI, Inc.

8. Le 18 janvier 2020, un article du New York Times intitulé *« The Secretive Company That Might End Privacy as We Know It »* révélait au monde l'existence de Clearview.[6] Avant cet article, Clearview avait intentionnellement opéré dans le secret, tout en offrant son produit à « plus de 600 organismes chargés de l'application de la loi » et à « au moins un petit nombre d'entreprises à des fins de sécurité ». À la suite de ces « révélations », des organisations et des autorités de contrôle aux États-Unis et dans le monde ont commencé à examiner de près les pratiques de Clearview.

9. Aux États-Unis, « huit actions putatives ont été intentées dans les jours qui ont suivi la publication de l'article du Times, et d'autres ont suivi ».[7] En raison de l'absence d'une loi fédérale américaine sur la protection de la vie privée, ces actions ont été intentées dans différents États en vertu de la législation de ces derniers. L'une de ces actions a été intentée en mai 2020 par l'ACLU dans l'Illinois[8] en vertu de la loi sur la confidentialité des informations biométriques de cet État (BIPA), qui réglemente la collecte et l'utilisation des informations biométriques. Une autre a été lancée en février 2021 en Californie par des militants des libertés civiles et des associations de défense des droits des immigrants, au motif que les pratiques de Clearview violent diverses interdictions municipales concernant l'utilisation par le gouvernement de technologies de reconnaissance faciale.[9]

10. Au Canada, le Commissariat à la protection de la vie privée (ci-après « **CPVP** »), en collaboration avec les organismes de surveillance provinciaux et territoriaux en matière de protection de la vie privée, a ouvert une enquête sur les pratiques de Clearview en février 2020. Le CPVP a publié son rapport de conclusions le 2 février 2021, dans lequel il recommande que Clearview : (i) cesse d'offrir son dispositif de reconnaissance faciale aux clients au Canada; (ii) mette fin à la « collecte, à l'utilisation et à la communication d'images et de matrices faciales biométriques recueillies auprès d'individus au Canada »; et (iii) supprime « les images et les matrices faciales biométriques recueillies auprès d'individus au Canada qu'elle a en sa possession ».[10]

11. Au Royaume-Uni et en Australie, les autorités de protection des données ont ouvert une enquête conjointe sur les « pratiques de traitement des données personnelles » de Clearview en juillet 2020.[11]

---

[6] Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It' (The New York Times, 18 janvier 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[7] Sam Jungyun Choi et al, 'Clearview AI revelations spark action on use of facial recognition', Privacy Laws & Business International Report (août 2020), https://www.cov.com/-/media/files/corporate/publications/2020/08/clearview-ai-revelations-spark-action-on-use-of-facial-recognition.pdf.
[8] ACLU, 'ACLU sues Clearview AI' (28 mai 2020), https://www.aclu.org/press-releases/aclu-sues-clearview-ai.
[9] CNN Business, 'Clearview AI sued in California by immigrant rights groups, activists' (10 mars 2021), https://edition.cnn.com/2021/03/09/tech/clearview-ai-mijente-lawsuit/index.html.
[10] CPVP (n 4.
[11] Information Commissioner's Office, 'The Office of the Australian Information Commissioner and the UK's Information Commissioner's Office open joint investigation into Clearview AI Inc.' (9 juillet 2020), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc.

12. Au sein de l'UE, des actions disparates ont été entreprises dans différents pays. En Allemagne, un particulier a obtenu de l'autorité de protection des données de Hambourg une ordonnance exigeant que Clearview supprime la valeur de hachage associée aux images de son visage.[12] La décision s'est limitée au cas individuel en question et n'a pas exigé la cessation des activités de Clearview dans cette juridiction. En Suède, l'Autorité suédoise pour la protection de la vie privée a estimé en février 2021 que la police suédoise avait illégalement utilisé les services de Clearview et traité des données personnelles en violation de la loi suédoise sur les données en matière pénale, la loi suédoise transposant la directive Police-Justice.[13] D'autres pays ont également ouvert des enquêtes sur les pratiques de Clearview, comme l'Italie.[14]

13. Le Comité européen de la protection des données (ci-après « **EDPB** »), suite à des questions de membres du Parlement européen soulevant des inquiétudes concernant Clearview, a publié une évaluation préliminaire le 10 juin 2020.[15] Cette évaluation s'est concentrée sur « la conformité et la licéité du traitement résultant de l'utilisation éventuelle par les forces de l'ordre de l'UE d'un service tel que celui proposé par Clearview AI », faisant état de doutes sérieux.

14. Le nombre de différents cas soulevés en Europe et ailleurs témoigne d'une préoccupation vive et généralisée de la part des particuliers et des autorités de contrôle concernant les pratiques de Clearview. Pourtant, à ce jour, aucun effort n'a été consacré à l'adoption d'une approche coordonnée de ce problème intrinsèquement mondial. Une approche coordonnée est attendue depuis trop longtemps en Europe, où l'on se targue de posséder l'un des cadres de protection de la vie privée et des données les plus exigeants au monde. En effet, une approche fragmentée nuirait à la valeur et à la force du RGPD et de la directive Police-Justice, censés apporter le même niveau de protection de la vie privée à tous les résidents européens.

B. Le traitement effectué par Clearview est soumis au RGPD et à la directive Police-Justice.

15. PI soutient que le comportement du responsable du traitement relève de l'article 3, paragraphe 2, du RGPD, étant donné que Clearview a été, à plusieurs reprises, citée comme offrant ses services à la fois à des entités privées et à des autorités répressives dans l'UE, et qu'elle s'est engagée dans le suivi du comportement des personnes concernées au sein de l'UE en collectant leurs données personnelles. En outre, le site internet de la société et

[12] noyb, 'Clearview AI's biometric photo database deemed illegal in the EU, but only partial deletion ordered' (28 janvier 2021), https://noyb.eu/en/clearview-ai-deemed-illegal-eu.
[13] GDPRhub, 'IMY - DI-2020-2719' (11 February 2021), https://gdprhub.eu/index.php?title=IMY_-_DI-2020-2719.
[14] Wired, 'Il Garante italiano della privacy indaga sulla più controversa società di riconoscimento facciale al mondo' (15 avril 2021), https://www.wired.it/attualita/tech/2021/04/15/riconoscimento-facciale-garante-privacy-clearview-ai/?refresh_ce=.
[15] EDPB, Lettre aux membres du Parlement européen (Ref : OUT2020-0052, 10 juin 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_fr.pdf.

son traitement de l'exercice des droits des personnes concernées confirment que la société a précédemment agi comme étant soumise aux obligations imposées par le RGPD.

Le ciblage des clients effectué par Clearview relève de l'article 3 paragraphe 2 point a) du RGPD.

16. Tout d'abord, en février 2020 le site internet BuzzFeed News rapportait que, selon des documents consultés par sa rédaction, Clearview aurait démarché « des services répressifs nationaux, des organes gouvernementaux et des forces de police ou de gendarmerie en Belgique, au Danemark, en Finlande, en France, en Irlande, en Italie, en Lettonie, en Lituanie, à Malte, aux Pays-Bas, au Portugal, en Slovénie, en Espagne et en Suède »,[16] offrant ainsi ou ayant l'intention d'offrir ses services en France comme dans d'autres pays de l'UE.

17. Deuxièmement, il est clair que le responsable du traitement a eu l'intention d'offrir ses services et d'en faire la promotion en Europe, en ciblant potentiellement tant des entités privées que des services répressifs nationaux comme clients. Par exemple, un document obtenu par BuzzFeed News via une demande de communication de documents publics a révélé que Clearview a vanté une « expansion internationale rapide » à des clients potentiels en utilisant une carte qui montre comment la société s'est développée ou prévoit de le faire.[17] Le document indique un certain nombre de pays de l'UE comme clients existants ou cibles.

18. Ces rapports et documents attestent d'un « comportement du responsable du traitement » démontrant son « intention d'offrir des biens ou des services à une personne située sur le territoire de l'Union », un élément clé pour déterminer si le critère de ciblage de l'article 3, paragraphe 2, point a), est rempli.[18]

Le traitement de données à caractère personnel par Clearview relève de l'article 3 paragraphe 2 point b) du RGPD.

19. Troisièmement, les réponses reçues de Clearview aux demandes d'accès des personnes concernées soumises en vertu de l'article 15 du RGPD montrent que la société a collecté des données personnelles de personnes concernées se trouvant dans l'UE et les a traitées d'une manière qui relève de l'application de l'article 3 paragraphe 2 point b) du RGPD. Le 16 avril 2020, un membre du personnel de PI, [redacted], a soumis une demande de droit d'accès à Clearview par courrier électronique, demandant « une copie de toutes [ses] données personnelles [que Clearview]

[16] BuzzFeed News (27 février 2020) (n 2.
[17] BuzzFeed News, 'Clearview AI Wants To Sell Its Facial Recognition Software To Authoritarian Regimes Around The World' (5 février 2020), https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22.
[18] EDPB, « Lignes directrices 3/2018 sur le champ d'application territorial du RGPD (article 3) version 2.1 » (12 novembre 2019), https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf.

traite » et a réclamé des réponses à une série de questions au titre de l'article 15 du RGPD. Une copie de la correspondance de [redacted] avec Clearview en relation avec cette demande de droit d'accès est reproduite à la Pièce n°1 de la présente réclamation. La réponse que [redacted] a reçue comprenait un fichier PDF contenant 3 photos de lui-même assorties d'un lien vers leur page internet d'origine, ainsi qu'une brève description de la troisième photo qui y était associée à son emplacement d'origine. Elle comportait également un lien vers une page internet intitulée « Clearview Data Policy », apparemment en réponse aux questions supplémentaires de [redacted], mais qui ne répondait pas à toutes ces questions.[19] De même, une demande de droit d'accès soumise par [redacted], également membre du personnel de PI (résidente du Royaume Uni et de nationalité française), a conduit Clearview à fournir un fichier PDF contenant 8 photos d'elle-même et les métadonnées associées (y compris son nom), ainsi que la photo et le nom d'une autre personne apparemment inclus par erreur (expurgés aux fins de la présente réclamation) (voir Pièce n°2).

20. La réponse de Clearview démontre que la société collecte et traite systématiquement, par le biais de son algorithme de reconnaissance faciale, les données à caractère personnel de toute personne ayant des images de son visage en ligne, ce qui inclut nécessairement les résidents de l'UE.[20] Cette pratique équivaut à un suivi du comportement des personnes concernées dans l'UE – elle tombe sous le coup de l'exigence du considérant 24 du RGPD selon lequel :

> *afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur l'internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit*.

21. Quatrièmement, l'avis du Groupe de travail « Article 29 » (« **G29** ») sur les aspects de la protection des données liés aux moteurs de recherche a conclu que « La directive sur la protection des données (95/46/CE) s'applique généralement au traitement de données à caractère personnel effectué par les moteurs de recherche, même lorsque leur siège se trouve en dehors de l'EEE ».[21] PI note que les principes d'applicabilité de la directive sur la protection des données (95/46/CE) étaient à cet égard les mêmes que ceux du RGPD. Le fait que Clearview fonctionne effectivement comme un moteur de

[19] Politique de données de Clearview. https://staticfiles.clearview.ai/clearview_data_policy.html.
[20] Nous avons connaissance d'un certain nombre de résidents français dont les données personnelles ont été traitées par Clearview, comme le confirment des demandes d'accès non effectués pour le compte de PI. Voir par exemple Jumbo Blog, 'Jumbo Privacy brings a formal RGPD complaint against Clearview' (14 juillet 2020), https://blog.jumboprivacy.com/jumbo-privacy-brings-a-formal-complaint-against-clearview.html.
[21] Groupe de Travail Article 29 sur la Protection des Données, « Avis 1/2008 sur les aspects de la protection des données liées aux moteurs de recherche » (00737/FR WP 148, 4 Avril 2008), p.27.

recherche qui fouille le web pour trouver des visages place ses activités dans le champ d'application du RGPD, malgré son absence d'établissement dans l'UE.

22. Cinquièmement, le traitement de données à caractère personnel de personnes concernées résidant dans l'UE par le responsable du traitement est indiqué par les éléments suivants provenant du site internet/de la plateforme accessible en ligne du responsable du traitement : (a) une référence est faite aux transferts internationaux dans une version récente de la politique de confidentialité du responsable du traitement : « Lorsque des données à caractère personnel sont transférées en dehors de l'EEE, nous mettrons en place des garanties appropriées pour nous assurer que ce transfert est effectué conformément aux règles applicables en matière de protection des données »[22] ; et (b) des références explicites au « Règlement général sur la protection des données » sont faites dans les conditions de service et la politique de confidentialité du responsable du traitement.[23]

23. Sixièmement, suite à une plainte déposée par une personne concernée résidant à Hambourg, le Commissaire de Hambourg pour la protection des données et la liberté d'information (ci-après le « **HmbBfDI** ») a communiqué le 27 janvier 2021 son intention d'ordonner à Clearview de prendre certaines mesures pour supprimer les données de la personne concernée. Le HmbBfDI a affirmé sa propre compétence et son application du RGPD après avoir conclu que Clearview suit effectivement le comportement des personnes concernées dans l'Union, en notant notamment que « l'objectif de l'entreprise est de pouvoir identifier les individus. Cette identification est possible en stockant les publications/profils/comptes des utilisateurs liés à une photographie, comme c'est le cas sur les réseaux sociaux, les forums ou les blogs, en établissant un profil, ou du moins en étant capable d'établir le profil d'un individu donné à tout moment. Cette utilisation ultérieure de techniques de traitement de données à caractère personnel visant au profilage est un indicateur déterminant ».[24]

24. Dans une affaire similaire à la présente, concernant la récolte de données personnelles par un responsable de traitement sans établissement dans l'UE, l'autorité de protection des données néerlandaise (« **Autoriteit Persoonsgegevens** ») a aussi affirmé sa propre compétence à propos des pratiques de locatefamily.com, qui récolte et partage des adresses et des noms de résidents européens.[25]

25. Nous estimons que la CNIL devrait arriver à une conclusion similaire à celles du HmbBfDI et de la Autoriteit Persoonsgegevens quant à l'applicabilité du RGPD.

---

[22] Clearview AI, Inc. Politique de confidentialité (version 1, dernière mise à jour le 29 janvier 2020), https://clearview.ai/privacy/privacy_policy.
[23] Clearview AI, Inc. Conditions de service, https://clearview.ai/help/tos.
[24] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (n 4).
[25] Autoriteit Persoonsgegevens, Décision du 10 Décembre 2020 contre locatefamily.com, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20210512_boetebesluit_ap_locatefamily.pdf.

26. Enfin, une version précédente de la politique de confidentialité de Clearview montrait que la société se soumettait ouvertement à la juridiction des autorités de protection des données de l'EEE : « Les résidents de l'Espace économique européen ou de la Suisse qui souhaitent déposer une plainte ou chercher à résoudre un litige lié au traitement des données personnelles par Clearview AI peuvent introduire gratuitement un recours en contactant l'autorité de protection des données (APD) appropriée dans leur pays respectif. »[26] Cette politique de confidentialité a été remplacée en mars 2021 par une version qui prend soin de ne pas faire référence aux résidents de l'EEE ou à la législation européenne[27], pour semble-t-il chercher à échapper à cet argument. A la date de cette réclamation, la version précédente de la politique de confidentialité, ainsi qu'un « Formulaire d'accès aux données UE/R-U/Suisse » et un formulaire « Opposition UE/R-U/Suisse/Australie » sont toujours disponibles en ligne, bien que déréférencés du site internet de Clearview.[28] Ces deux formulaires étaient préalablement disponibles sur une page nommée « Formulaires Requêtes Vie Privée ».[29] Comme rien ne prouve que Clearview a changé ses pratiques ni cessé de traiter les données personnelles des résidents de l'UE, nous ne voyons aucune raison de penser que celles-ci ne tomberaient plus sous le champ d'application du droit européen. Dans tous les cas, les données récoltées lorsque la précédente version de la politique de confidentialité était en vigueur sont soumises à la juridiction déclarée dans cette précédente version.

27. Pour les raisons exposées ci-dessus, PI estime que la CNIL doit considérer que le comportement du responsable du traitement entre dans le champ d'application de l'article 3, paragraphe 2, du RGPD. Clearview se voit donc, en outre, dans l'obligation de désigner un représentant dans l'Union, comme prévenu à l'article 27, paragraphe 1 du RGPD. Aucune des exceptions de l'article 27, paragraphe 2 ne peut s'appliquer.[30]

28. En outre, à la lumière des débats actuels et des propositions de réglementation de la surveillance biométrique de masse[31], PI soutient que les lois existantes sur la vie privée et la réglementation sur la protection des données sont tout à fait suffisantes pour juger illégales les pratiques de Clearview. Une réglementation de la surveillance biométrique de masse serait en effet nécessaire pour fournir une clarté juridique sur l'utilisation de la technologie de reconnaissance faciale sur la voie publique dans des cas limités et individuels.

---

[26] Clearview AI, Inc. Politique de confidentialité (version 1) (n 22).
[27] Clearview AI, Inc. Politique de confidentialité (version 2, dernière mise à jour le 20 mars 2021), https://clearview.ai/privacy-policy.
[28] Voir EU/UK/Switzerland Data Access Form, https://clearviewai.typeform.com/to/ePcsEp et EU/UK/Switzerland/Australia Opt-Out, https://clearviewai.typeform.com/to/zqMFnt.
[29] Voir Clearview AI, 'Privacy Request Forms', disponible sur la Wayback Machine Internet Archive, https://web.archive.org/web/20210303033642/https://clearview.ai/privacy/requests.
[30] Pour des décisions similaires sur l'absence de représentant, voir Autoriteit Persoonsgegevens (n 25), et Commission nationale pour la protection des données du Luxembourg, décision du 4 février 2020, https://gdprhub.eu/index.php?title=CNPD_-_3018).
[31] Commission européenne, « Proposition de règlement établissant des règles harmonisées en matière d'intelligence artificielle (loi sur l'intelligence artificielle) », COM(2021) 206 final (21 avril 2021).

Mais le traitement de masse des données biométriques par une société privée relève entièrement de la législation existante, qui a précisément été conçue pour protéger les citoyens européens contre ce type de pratiques.

C. Pourquoi la CNIL devrait traiter cette réclamation

29. Dans une déclaration du 14 juillet 2020, la société Jumbo Privacy a signalé le dépôt d'une plainte visant Clearview, suite à l'échec des efforts déployés par l'un des membres de son personnel dans l'exercice de ses droits en tant que personne concernée.[32] PI espère sincèrement que les analyses techniques et juridiques détaillées des pratiques de Clearview qui ont alimenté la présente réclamation seront utiles à toute enquête en cours.

30. PI s'inquiète de l'offre des services de Clearview à des clients privés ou à des autorités répressives, car le fonctionnement et l'utilisation de ces services peut fondamentalement entraver les droits des individus à la protection des données. Ceux-ci perpétuent précisément les préjudices que la législation sur la protection des données s'évertue à remédier. Laissés non sanctionnées, ces pratiques auront de sérieuses conséquences pour notre société. À l'ère digitale, ces conséquences consistent en un effet dissuasif sur la participation des citoyens dans les processus démocratiques à travers Internet, en des contraintes sur le développement de leurs identités socio-politiques, et en des préjudices bien réels et physiques tels qu'une vulnérabilité au « stalking » et une incapacité à mener des activités quotidiennes sans la menace d'une surveillance constante.

31. En outre, ayant déposé des demandes similaires auprès d'un certain nombre d'autorités de protection des données de l'UE[33], PI soutient qu'il serait avantageux pour la CNIL de s'emparer des mécanismes de coopération et de cohérence prévus par les articles 60 à 62 du RGPD. La dernière évaluation du RGPD par la Commission européenne[34] remarque que « les autorités de protection des données n'ont pas encore fait pleinement usage des outils fournis par le RGPD, tels que les opérations conjointes pouvant conduire à des enquêtes conjointes ». PI soutient que les enquêtes visant Clearview AI bénéficieraient grandement d'une coopération transfrontalière et qu'une mise en œuvre efficace des textes requiert une approche transfrontalière cohérente. Comme nous l'expliquons plus en détail dans la section V.D ci-dessous, les pratiques de Clearview menacent le caractère ouvert d'Internet et les nombreuses libertés qu'il habilite. En raison de la nature mondiale d'Internet, la préservation de ces caractéristiques essentielles nécessite une approche internationale ayant effet à l'échelle la plus large possible.

---

[32] Jumbo Blog (n 20).

[33] [Italie, Grèce, Allemagne, Autriche et France.]

[34] Commission européenne, « Communication de la Commission au Parlement européen et au Conseil - La protection des données, pilier de la responsabilisation des citoyens, et l'approche de l'UE en matière de transition numérique - deux ans d'application du règlement général sur la protection des données » (COM(2020)0264) (24 juin 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264.

V. Cadre juridique et préoccupations : Les opérations de traitement de Clearview AI, Inc. (RGPD)

32. Cette section de la présente réclamation expose les préoccupations de PI concernant la première étape de l'interaction de Clearview avec les personnes concernées dans l'UE, à savoir le traitement initial des données personnelles par la collecte, le stockage et l'extraction des caractéristiques du visage. Notre analyse juridique et nos préoccupations sont fondées sur les enquêtes de PI réalisées à partir de sources accessibles au public concernant la technologie de Clearview, éclairées par l'expertise technologique et juridique de PI. Les principales préoccupations sont que (i) Clearview traite à la fois des données à caractère personnel non sensibles et des catégories particulières de données, en l'absence de toute base légale valable, et (ii) ce traitement s'inscrit en violation de plusieurs autres principes du RGPD.

33. Après avoir démontré que Clearview traite des données à caractère personnel (ci-après « **DACP** ») et des catégories particulières de données personnelles (section A, cette section de la présente réclamation exposera les différentes violations du RGPD dans les pratiques de collecte, de stockage et d'identification par Clearview, qui ne respectent pas les principes de protection des données suivants prévus à l'article 5 du RGPD :

    (a) Principe 1 – Licéité, loyauté et transparence
        i. Transparence (section B)
        ii. Loyauté (section C)
        iii. Licéité et base légale de traitement en vertu des articles 6 et 9 du RGPD (intérêts légitimes et catégories particulières de DACP) (section D).
    (b) Principe 2 - Limitation des finalités (section **Error! Reference source not found.**)

A. Clearview traite des données à caractère personnel et des catégories particulières de données

Clearview traite des DACP telles que définies par l'article 4 paragraphe 1 du RGPD.

34. Se fondant sur la description technique du produit de Clearview développée dans la section III ci-dessus, PI soutient que la société Clearview effectue des opérations de « traitement de données à caractère personnel, automatisé en tout ou en partie », comme le prévoit l'article 2, paragraphe 1, du RGPD.

35. Premièrement, les images que Clearview collecte à partir de sources accessibles au public sur Internet sont des DACP. Les photographies entrent tout à fait dans la définition des données à caractère personnel au sens de l'article 4 paragraphe 1 du RGPD, notamment tel qu'interprété à l'aide du considérant 26 du règlement : « Il y a lieu d'appliquer les principes relatifs à la protection des données à toute information concernant une personne physique identifiée ou identifiable. […] Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens

raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement ». En raison de l'unicité d'un visage, la photographie d'un visage permet nécessairement, par reconnaissance « humaine », l'identification d'un individu. Comme le démontre la technologie de Clearview, elle permet aussi nécessairement l'identification par reconnaissance machine.

36. Une telle conclusion est également conforme à la jurisprudence de la Cour de justice de l'Union européenne (ci-après « **CJUE** »). Cette dernière a jugé que « l'image d'une personne enregistrée par une caméra constitue une donnée à caractère personnel au sens de [l'article 2, sous a), de la directive 95/46] dans la mesure où elle permet d'identifier la personne concernée ».[35] La définition des DACP au sens de la directive 95/46 est, en substance, la même que celle contenue dans l'article 4, paragraphe 1, du RGPD.

37. Deuxièmement, les métadonnées que Clearview collecte, stocke et associe également aux images peuvent contenir des DACP. Comme on peut le voir dans les résultats d'une demande de droit d'accès envoyée par [redacted], membre du personnel de PI (Pièce n°2), l' « index des images » (*Image Index*) fourni sous les résultats de recherche de visages (*Face Results*) contient des descriptions de l'image et/ou de la page internet où l'image a été trouvée, et comporte souvent des DACP telles que des noms de personnes – y compris celles d'une personne différente, que nous avons expurgées. Cela confirme également que les photos collectées par Clearview sont des DACP, car elles peuvent permettre « indirectement » l'identification d'une personne concernée – le responsable du traitement dispose « des moyens susceptibles d'être raisonnablement mis en œuvre […] pour identifier la personne concernée », ce qui rend la personne indirectement identifiable, conformément à l'arrêt *Breyer* de la CJUE.[36]

38. Troisièmement, en septembre 2019 au Royaume Uni, dans le premier jugement de grande ampleur traitant de l'utilisation en direct d'une technologie de reconnaissance faciale automatisée par des services de police appelée « AFR locate », une Cour divisionnaire est allée jusqu'à accepter que toute donnée biométrique permettant « l'identification immédiate d'une personne » comprenait des DACP.[37] Comme l'a souligné la Cour :

> *Les membres du public filmés par les caméras de vidéosurveillance sont suffisamment individualisés car l'équipement AFR Locate capture des images de leurs visages, ces informations sont traitées pour extraire des données biométriques, qui sont elles-mêmes traitées en étant comparées aux informations tirées de la liste de personnes recherchées. Par nature, les données biométriques du visage sont des informations concernant une personne physique. Cette personne est identifiable au sens de la définition de la directive de 1995 et de la loi sur la protection des données de 1998*

[35] Affaire C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014] ECLI:EU:C:2014:2428, point 22.
[36] Affaire C-582/14 *Patrick Breyer contre Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779, point 48.
[37] *R (Bridges) v Chief Constable of South Wales Police* ([2019] EWHC 2341 (Admin)), paragraphe 125.

[UK Data Protection Act 1998] *parce que ces données biométriques du visage sont utilisées pour distinguer cette personne de toute autre personne afin que le processus de comparaison puisse avoir lieu.* [38]

39. Si cet arrêt portait sur le déploiement de la reconnaissance faciale automatisée par le biais de caméras dans des lieux publics, PI soutient que la même conclusion s'applique à la technologie de reconnaissance faciale utilisée par Clearview, celle-ci permettant également l'identification immédiate de personnes physiques.

40. Quatrièmement, ces données personnelles sont collectées, stockées, structurées par indexation via des vecteurs, et récupérées lorsqu'un utilisateur effectue une recherche. Toutes ces opérations relèvent de la définition de « traitement » au titre de l'article 4, paragraphe 2, du RGPD.

Clearview traite des données biométriques telles que définies par l'article 4 paragraphe 14 du RGPD.

41. En vertu de l'article 4 paragraphe 14 du RGPD, les « données biométriques » sont définies comme « données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, **telles que des images faciales**. »

42. Clearview traite donc des données biométriques à au moins deux égards :

    (a) Les images faciales que la société collecte à partir de sources accessibles en ligne sont des données biométriques.
    (b) Une fois les vecteurs créés, ils deviennent eux-mêmes des données biométriques, car ce sont des données résultant d'un « traitement technique spécifique, relatives aux caractéristiques physiques [...] d'une personne physique, qui permettent ou confirment son identification unique ».

Clearview traite des catégories particulières de données à caractère personnel telles que définies par l'article 9 paragraphe 1 du RGPD.

43. Clearview traite systématiquement des catégories particulières de DACP telles que définies par l'article 9 paragraphe 1 du RGPD. En vertu de l'article 9 paragraphe 1, les catégories particulières de DACP sont définies comme incluant « les données biométriques aux fins d'identifier une personne physique de manière unique ». Selon le considérant 51 du RGPD, « [l]e traitement des photographies ne devrait pas systématiquement être considéré comme constituant un traitement de catégories particulières de données à caractère personnel, étant donné que celles-ci ne relèvent de la définition de données biométriques que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne

[38] Id., paragraphe 124.

physique ». S'il en ressort que les photographies de visages que Clearview collecte à partir de sources accessibles en ligne ne sont pas nécessairement des catégories particulières de DACP, il est également clair que ces photographies le deviennent dès qu'elles sont traitées à l'étape 3 de la construction de la base de données de Clearview. La numérisation de chaque visage, l'extraction de ses caractéristiques faciales d'identification unique et la traduction de ces caractéristiques en vecteurs consistent en « un traitement technique spécifique » permettant l'identification unique d'une personne physique.

44. Cette conclusion est également conforme aux conclusions de la Cour divisionnaire dans l'affaire *Bridges*, où il a été jugé que « le fonctionnement de l'outil « AFR Locate » implique le traitement sensible des données biométriques de » personnes, indépendamment du fait que leurs images figurent ou non sur des listes de personnes recherchées : [39]

> *le logiciel AFR prend une image numérique et la traite par le biais d'un algorithme mathématique pour produire un modèle biométrique (c'est-à-dire du membre du public qui n'est pas sur la liste de personnes recherchées) qui est ensuite comparé à d'autres modèles biométriques (c'est-à-dire de ceux qui sont sur cette même liste) afin de fournir des informations sur la ressemblance d'une image avec l'autre. Ce processus de comparaison ne peut avoir lieu que si chaque modèle identifie de manière unique la personne à laquelle il se rapporte. Bien que l'objectif général de la police du Sud du Pays de Galle soit d'identifier les personnes figurant sur la liste de personnes recherchées, pour atteindre cet objectif général, les informations biométriques des membres du public doivent également être traitées de manière à ce que chacun d'entre eux soit également identifié de manière unique, en l'occurrence pour réaliser une comparaison. Cela suffit à faire entrer le traitement de leurs données biométriques dans le champ d'application de l'article 35 paragraphe 8 point b) de la loi britannique sur la protection des données de 2018.*[40]

45. En outre, les métadonnées collectées, stockées et associées aux images faciales peuvent contenir des DACP révélant « l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale », qui sont des catégories particulières de données. Par exemple, les images faciales peuvent être trouvées sur le site internet d'une association cultuelle ou sur celui d'un syndicat, ce qui permet d'associer des personnes identifiables à ces caractéristiques.

46. Il convient également de noter que Clearview traite les données personnelles d'enfants dont les images faciales sont disponibles en ligne[41] et dont le

---

[39] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin), paragraphe 133.
[40] Id.
[41] Voir la lettre d'Edward J. Markey (sénateur des États-Unis) à M. Hoan Ton-That (3 mars 2020), p. 2, : https://www.markey.senate.gov/imo/media/doc/Markey%20Letter%20-%20Clearview%20II%203.3.20.pdf, citant Kashmir Hill et Gabriel J.X. Dance, 'Clearview's Facial Recognition App Is Identifying Child Victims of Abuse',

traitement est soumis à des restrictions encore plus importantes par le RGPD.[42] Le 17 octobre 2019, la CNIL observait que « les risques majeurs d'atteinte à la vie privée et aux libertés individuelles des personnes concernées [que présentent les dispositifs de reconnaissance faciale] se trouvent accrus lorsque [ceux-ci] sont appliqués à des mineurs, qui font l'objet d'une protection particulière dans les textes nationaux et européens ». [43]

B. Transparence et droit à l'information

47. La transparence est une composante essentielle du premier principe de protection des données, énoncé à l'article 5, paragraphe 1, point a), du RGPD et soutenu par le droit à l'information prévu aux articles 13 et 14. Le considérant 60 du RGPD prévoit que « [l]e principe de traitement loyal et transparent exige que la personne concernée soit informée de l'existence de l'opération de traitement et de ses finalités. » En vertu de l'article 14, paragraphe 3, point a), lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, comme c'est le cas pour le traitement effectué par Clearview, le responsable du traitement doit fournir des informations à la personne concernée « dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois ».

48. Clearview affiche sur son site internet une politique de confidentialité (ci-après la « **Politique** »)[44] qui a été mise à jour en mars 2021 à partir d'une version antérieure destinée à un public mondial.[45] La nouvelle version a supprimé la référence aux résidents de l'Espace économique européen ou de la Suisse. Pourtant, elle s'applique expressément aux « photos accessibles au public sur Internet » et à l'extraction de « la géolocalisation et des mesures des caractéristiques faciales des personnes figurant sur les photos » – ce qui signifie qu'elle s'applique nécessairement à toutes les personnes dans le monde qui, sciemment ou non, ont leurs images faciales hébergées sur des zones accessibles au public sur Internet, et donc aux résidents de l'UE.

49. Clearview ne remplit pas les exigences de transparence pour au moins deux raisons. Premièrement, Clearview n'informe jamais les internautes que la société traite leurs données personnelles, de sorte que les personnes concernées n'ont jamais la possibilité de lire la politique de confidentialité de Clearview que ce soit avant ou après le traitement de leurs données personnelles. Selon les lignes directrices du G29 sur la transparence[46], « Un aspect primordial du principe de transparence [...] est que la personne

---

(New York Times, 7 février 2020), https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html.

[42] Par exemple, les articles 8, 12, paragraphe 1, et 17, paragraphe 1, point f), et le considérant 38.

[43] CNIL, « Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position », 29 octobre 2019, https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

[44] Politique de confidentialité de Clearview (version 2) (n 27).

[45] Politique de confidentialité de Clearview (version 1) (n 22).

[46] Groupe de travail Article 29 sur la protection des données, « Lignes directrices sur la transparence en vertu du règlement 2016/679 » (17/EN WP260 rev.01, adoptées le 29 novembre 2017, version révisée et adoptée le 11 avril 2018). https://www.cnil.fr/sites/default/files/atoms/files/wp260_guidelines-transparence-fr.pdf.

concernée devrait être en mesure de déterminer à l'avance ce que la portée et les conséquences du traitement englobent afin de ne pas être prise au dépourvu à un stade ultérieur quant à la façon dont ses données à caractère personnel ont été utilisées ». Dans le cas de Clearview, la surprise est totale : la seule façon pour une personne concernée de savoir que ses données ont été traitées est de prendre connaissance des divers reportages effectués par les médias sur le sujet et d'entrer en contact avec Clearview.

50. Deuxièmement, même si une personne était en mesure d'accéder à la politique de confidentialité de Clearview à un moment approprié, c'est-à-dire dès le stade de la collecte de ses données personnelles, Clearview fournit des informations incomplètes et trompeuses. Dans la section « Quelles sont les données que nous collectons ? », la société indique qu'elle « collecte des photos accessibles au public sur Internet » et qu'elle « peut extraire des informations de ces photos, y compris la géolocalisation et les mesures des caractéristiques du visage des personnes figurant sur les photos ». Cette déclaration est incomplète et trompeuse à deux égards : (1) elle présente l'extraction d'informations et la mesure des traits du visage comme une simple possibilité (en utilisant le mot « peut », qui devrait être évité dans les déclarations de confidentialité[47]), alors qu'il s'agit en réalité d'un processus automatique, et (2) elle omet divers autres types de DACP que Clearview collecte automatiquement, à savoir les noms et autres données obtenues à partir des adresses URL, des photos et des titres des pages internet traités.

51. En outre, cette nouvelle version de la politique de confidentialité de Clearview a supprimé les informations relatives aux bases légales sur lesquelles Clearview se fonde pour justifier le traitement des données personnelles. La version précédente de la politique de confidentialité de Clearview faisait référence à des bases légales spécifiques au RGPD telles que les intérêts légitimes ou le consentement explicite.[48] Encore une fois, dans ce qui peut être perçu comme un effort pour échapper au champ d'application du RGPD, Clearview a supprimé des informations essentielles qui doivent être fournies lors du traitement des données personnelles des résidents de l'UE.

52. Dans plusieurs déclarations publiques[49], Clearview a semblé considérer que tout droit à l'information était oblitéré par le fait que les données à caractère personnel obtenues étaient accessibles au public, et que les personnes concernées auraient donc « renoncé » à ce droit en acceptant tacitement que leurs images soient mises à la libre disposition du public en ligne. Cependant, comme la présente réclamation l'analysera et l'expliquera plus en détail aux paragraphes 91, il existe de nombreuses raisons pour lesquelles cela est faux. Il est donc inacceptable pour Clearview de prétendre que les personnes sont pleinement informées et consentent à ce que leurs images faciales soient traitées de la sorte.

---

[47] Art 29 Lignes directrices du GT sur la transparence (n. 46), paragraphe 13.
[48] Politique de confidentialité de Clearview (version 1) (n 22).
[49] Par exemple, la chaîne YouTube CNN Business, 'Clearview AI's founder Hoan Ton-That speaks out [Extended interview]' (6 mars 2020), https://www.youtube.com/watch?v=q-1bR3P9RAw.

53. Ce manque de transparence, qui constitue en soi une violation du RGPD, implique également qu'une écrasante majorité de personnes concernées n'ont pas connaissance du traitement de leurs données personnelles par Clearview et ne peuvent donc exercer aucun de leurs droits en tant que personnes concernées découlant de ce traitement.

C. La loyauté et les attentes raisonnables des personnes concernées

54. La loyauté est une autre composante du premier principe de protection des données énoncé à l'article 5, paragraphe 1, point a), du RGPD. Un aspect essentiel de la loyauté est que le traitement de DACP doit être conforme aux attentes raisonnables des personnes. Pour l'ICO, « la loyauté signifie que les données à caractère personnel doivent être traitées uniquement de telle sorte que les personnes peuvent s'y attendre raisonnablement et ne pas être utilisées d'une façon qui aurait des effets préjudiciables injustifiés sur elles ».[50] Pour le Conseil d'Etat, le principe de loyauté est un corollaire des principes généraux de la responsabilité : « collecter des données de manière déloyale, c'est surprendre la confiance de la personne concernée et commettre ainsi une faute à son égard »[51].

55. Tenir compte des attentes raisonnables de la personne concernée en matière de respect de la vie privée est également un principe clé de la jurisprudence de la Cour européenne des droits de l'homme (ci-après la « **CEDH** »), qui sert à déterminer s'il y a eu ingérence dans la vie privée d'un individu en vertu de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (la « **CESDH** »). La CEDH a, en plusieurs occasions, examiné si un individu « pouvait raisonnablement s'attendre à ce que sa vie privée soit protégée et respectée ».[52] Dans sa jurisprudence, la Cour a souligné qu'aucune personne ne pouvait raisonnablement s'attendre à ce que des séquences décrivant des aspects sensibles de sa vie privée soient ultérieurement diffusées dans les médias, même si ses actes sont « à la disposition du grand public »[53], et que l'utilisation d'équipements photographiques pour capturer et traiter les données biométriques d'une personne à des fins autres que celles initialement prévues par celle-ci ne peut pas relever de ses attentes raisonnables en matière de vie privée.[54]

56. PI soutient que les attentes raisonnables des personnes concernées sont manifestement bafouées par les pratiques de Clearview. Dans sa récente décision, la CPVP a estimé que « les personnes qui ont publié leurs images en

---

[50] Traduit de l'anglais : 'fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.' ; ICO, 'Guide to the General Data Protection Regulation (RGPD) - Principle (a) : Légalité, équité et transparence'. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-RGPD/principles/lawfulness-fairness-and-transparency/#fairness.

[51] *Le Numérique et les droits fondamentaux*, 2014, p.173.

[52] *Barbulescu c. Roumanie* [GC] App no 1496/08 (CEDH, 5 septembre 2017), paragraphe 73.

[53] *Peck c. Royaume-Uni* App No 44647/98 (CEDH, 28 janvier 2003), paragraphes 61-62.

[54] *Perry c. Royaume-Uni* App No 63737/00 (CEDH, 17 juillet 2003), paragraphe 41.

ligne, ou dont les images ont été publiées par un ou plusieurs tiers, ne pouvaient raisonnablement s'attendre à ce que Clearview les recueille, utilise et communique à des fins d'identification ».[55] Ce constat est confirmé par une enquête menée par l'Agence européenne des droits fondamentaux (FRA), dans laquelle les citoyens européens ont été consultés sur leur volonté de partager différents types de données personnelles avec des agences gouvernementales et des entreprises privées.[56] Dans l'ensemble des 27 pays de l'UE, 94 % des personnes interrogées ont déclaré explicitement qu'elles n'étaient pas disposées à partager leurs images faciales avec des entreprises privées à des fins d'identification.

57. La pratique consistant à collecter et à traiter des données accessibles au public à partir de plateformes de réseaux sociaux, appelée « social media intelligence » (« **SOCMINT** ») ou « social media monitoring », a été décriée ces dernières années pour son incompatibilité avec les attentes raisonnables des personnes en matière de vie privée. Dans le cadre d'une consultation sur l'utilisation de la surveillance des réseaux sociaux par le Bureau européen d'appui en matière d'asile, le Contrôleur européen de la protection des données (« **CEPD** ») a estimé que la surveillance des réseaux sociaux « implique des utilisations de données à caractère personnel qui vont à l'encontre ou au-delà des attentes raisonnables des personnes. Ces utilisations ont souvent pour conséquence que les données personnelles sont utilisées au-delà de leur finalité initiale, de leur contexte initial et d'une manière que l'individu ne peut raisonnablement pas anticiper. » [57]

58. Le traitement effectué par Clearview est une forme particulièrement intrusive de surveillance des réseaux sociaux, qui va bien au-delà de la consultation et de l'analyse ponctuelles d'informations accessibles au public. La collecte, le stockage et le traitement automatiques de Clearview en vue de l'extraction d'identifiants biométriques sont encore plus éloignés de toute attente raisonnable des personnes concernées et ne sont donc en aucun cas conformes au principe de loyauté. L'application de la reconnaissance faciale à la collecte de données aggrave le problème : dans sa lettre au Parlement européen donnant un avis préliminaire sur l'utilisation de Clearview par les forces de l'ordre, l'EDPB a souligné que la technologie de reconnaissance faciale peut « affecter l'attente raisonnable des individus en matière d'anonymat sur la voie publique ».[58] En combinant la surveillance des réseaux sociaux et la technologie de reconnaissance faciale, le service offert par

[55] CPVP (n 4), Vue d'ensemble.
[56] Agence des droits fondamentaux de l'Union européenne, « Vos droits comptent : Protection des données et de la vie privée - Enquête sur les droits fondamentaux » (18 juin 2020). https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection#TabPubSharingdataonline1.
[57] Traduit de l'anglais 'involves uses of personal data that go against or beyond individuals' reasonable expectations. Such uses often result in personal data being used beyond their initial purpose, their initial context and in ways the individual could not reasonably anticipate.' ; EDPS, 'Formal consultation on EASO's social media monitoring reports (case 2018-1083)' (Brussels, D(2019) 1961), https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf.
[58] Traduit de l'anglais : 'affect individuals' reasonable expectation of anonymity in public spaces' ; 'Lettre de l'EDPB au Parlement européen (n 15), 10 juin 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf .

Clearview neutralise effectivement l'attente des individus au titre de laquelle leur vie et leur identité dans le monde physique ne peuvent être immédiatement reliées à leur vie et identité sur Internet.

Comparaison avec le moteur de recherche de Google

59. Dans divers rapports publics, Clearview a souvent comparé son service au moteur de recherche de Google, en faisant valoir que son service est simplement un « moteur de recherche de visages » au lieu d'un moteur de recherche traditionnel, utilisant des visages plutôt que des mots comme termes de recherche.[59] Cette comparaison semble destinée à montrer que l'outil de Clearview répondrait aux attentes raisonnables des personnes concernées en matière de respect de la vie privée, puisque chacun est conscient que ses données sont traitées par les moteurs de recherche. Toutefois, PI souhaite apporter quelques clarifications quant aux processus techniques effectués sur les plateformes de Google et de Clearview, avec pour objectif de démontrer que ceux-ci sont fondamentalement différents.

60. Les « moteurs de recherche » de Google et de Clearview effectuent tous deux trois actions distinctes :

    (a) *Crawling* – accès automatique à un site web et obtention de données de ce site ;
    (b) *Indexation* – téléchargement du contenu d'une page web vers le serveur du moteur de recherche, ajoutant ainsi du contenu à son « index » ; et
    (c) *Listing* – affichage du contenu correspondant dans les pages de résultats de recherche.

61. Au stade du *crawling*, le propriétaire d'un site Web peut utiliser un fichier robots.txt pour indiquer aux robots d'indexation comment explorer les pages de son site. Il s'agit d'un fichier texte qui permet aux administrateurs de sites internet d'indiquer à un moteur de recherche qu'ils ne souhaitent pas, par exemple, que le contenu de leur page soit indexé. D'un point de vue technique, respecter le fichier robots.txt est facultatif et celui-ci peut donc potentiellement être ignoré par les robots d'indexation. Des plateformes à l'image de LinkedIn ou Facebook ont inclus de tels fichiers sur leurs pages internet, et interdisent explicitement l'utilisation de robots d'indexation dans les conditions générales d'utilisation de leurs sites internet.

62. Google donne aux administrateurs de sites internet le contrôle des informations de leurs pages qui sont indexées et répertoriées dans ses résultats de recherche, avec la possibilité de les refuser complètement. Clearview a déclaré que son robot d'indexation d'images était configuré pour respecter les instructions présentes dans les fichiers robots.txt.[60] Cependant, la société a indexé du contenu provenant de YouTube, Facebook, Twitter et Instagram.[61]

[59] Par exemple, CNN Business, 'Clearview AI's founder Hoan Ton-That speaks out [Extended interview]' (n. 49.
[60] CPVP (n. 4), paragraphe 17.
[61] Hill (n 6).

Dans le cas de YouTube, la plateforme interdit explicitement la collecte automatisée de toute information susceptible d'identifier une personne, ainsi que le *scraping* de toute donnée, sauf par les « moteurs de recherche publics », tels que celui de Google.[62]

63. Clearview ne respecte donc pas les instructions interdisant le *crawling* comme le *scraping* du contenu de certains sites internet. Pour cette raison, la société a été poursuivie par plusieurs grandes plateformes pour violation de leurs conditions d'utilisation.[63] L'une des raisons pour lesquelles le *crawling* de Google est acceptable, alors que l'extraction par Clearview ne l'est pas, est que Google existe depuis les premiers jours du Web 2.0. Les utilisateurs de ce dernier ont développé du contenu et utilisé internet en sachant que Google existait et que le moteur de recherche allait explorer et indexer leur contenu. Clearview, en revanche, est intervenu plus de dix ans après l'essor des réseaux sociaux, en revendiquant la légitimité de l'extraction de toutes les données mises en ligne par les utilisateurs au cours de cette décennie et de leur traitement au moyen de technologies de reconnaissance faciale qui n'existaient pas il y a quelques années. Ces pratiques vont manifestement à l'encontre des principes de prévisibilité et d'attente légitime des personnes concernées.

64. La collecte généralisée et indifférenciée d'images faciales de personnes sur Internet ne répond donc pas aux attentes raisonnables des individus et viole le principe de loyauté. Ce dernier manquement est exacerbé par l'absence de transparence et le non-respect du droit à l'information des personnes, ainsi que par plusieurs autres violations de principes de protection des données, comme le précisera la présente réclamation.

D. Licéité et base légale de traitement

65. Le troisième élément du premier principe de protection des données énoncé à l'article 5, paragraphe 1, point a), du RGPD est la licéité, qui exige que les DACP soient traitées légalement. L'article 6 établit une liste exhaustive des bases légales sur le fondement desquelles les DACP peuvent être traitées.

66. En plus d'exiger une base légale en vertu de l'article 6, le traitement de « catégories particulières » de DACP est interdit à moins que l'une des conditions de la liste exhaustive figurant à l'article 9 paragraphe 2 du RGPD ne soit remplie. Étant donné que Clearview traite des données biométriques qualifiées de « catégories particulières » de données, la société devrait se prévaloir d'une base légale de traitement valide cumulativement en vertu de l'article 6 et de l'article 9 – plutôt qu'en application de l'une ou l'autre de ces

[62] YouTube FR, Conditions d'utilisation, https://www.youtube.com/t/terms.
[63] Alfred Ng et Steven Musil, 'Clearview AI hit with cease-and-desist from Google, Facebook over facial recognition collection' (CNET, 5 février 2020), https://www.cnet.com/news/clearview-ai-hit-with-cease-and-desist-from-google-over-facial-recognition-collection/.

dispositions.[64] Il ressort clairement de la version précédente de la politique de confidentialité de Clearview[65] que cette double exigence n'était pas bien assimilée par l'entreprise. Dans la section « Base légale du traitement », la société listait des bases légales pour le traitement des données personnelles (tirées de l'article 6) distinctes des bases légales nécessaires pour le traitement de catégories particulières de données (tirées de l'article 9). En outre, dans des reportages publics, la société semble être convaincue que l'argument « nous n'obtenons des données qu'à partir de sources accessibles au public » justifie à lui seul l'ensemble de ses traitements.

67. Cette réclamation va à présent analyser l'applicabilité des bases légales les plus pertinentes pour les opérations de traitement de Clearview en application des articles 6 et 9 du RGPD.

Intérêts légitimes - Article 6, paragraphe 1, point f) du RGPD

68. La principale base légale sur laquelle Clearview pourrait fonder ses opérations de traitement en vertu de l'article 6 du RGPD, et sur laquelle la société semble se fonder, est l' « intérêt légitime » (article 6, paragraphe 1, point f)). Cela ressort de l'inapplicabilité évidente d'autres bases légales, et du fait que dans la version précédente de sa politique de confidentialité[66], Clearview se fondait explicitement sur cette base légale : « le traitement est nécessaire aux intérêts légitimes de Clearview, et ne porte pas une atteinte excessive à vos intérêts ou à vos droits et libertés fondamentaux ». Les autres bases sur lesquelles la société a cherché à se fonder ne s'appliquaient qu'aux données relatives aux utilisateurs de ses services. Par exemple, la base légale « nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique » (article 6, paragraphe 1, point d)) ne pouvait potentiellement s'appliquer qu'à la dernière étape du traitement dans le cycle de vie de l'outil Clearview, c'est-à-dire lorsque le produit est utilisé par une autorité répressive dans le cadre d'une enquête pénale portant sur un crime ou un délit précis – l'entreprise ne saurait justifier l'ensemble du traitement antérieur au déclenchement d'une telle enquête.

69. Le considérant 47 du RGPD prévoit que les intérêts légitimes d'un responsable du traitement :

> *peuvent constituer une base juridique pour le traitement, à moins que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne prévalent, compte tenu* ***des attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement****. Un tel intérêt légitime pourrait, par exemple, exister lorsqu'il*

[64] Pour un soutien sans équivoque à cette vision « cumulative », voir G29, Avis 06/2014 sur la notion d'intérêts légitimes du responsable du traitement au titre de l'article 7 de la Directive 95/46/EC' (844/14/EN WP217 Adopted on 9 November 2014), p.14. Voir également Edward S Dove et Jiahong Chen, 'What does it mean for a data subject to make their personal data 'manifestly public' ? An analysis of RGPD Article 9(2)(e)' (2021) Vol. 00, No. 0, International Data Privacy Law, 1, 2.
[65] Politique de confidentialité de Clearview (version 1) (n 22).
[66] Id.

existe ***une relation pertinente et appropriée entre la personne concernée et le responsable du traitement dans des situations telles que celles où la personne concernée est un client du responsable du traitement*** *ou est à son service. En tout état de cause, l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de* ***déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de*** *la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée* (gras ajouté).

70. Si la base de l' « intérêt légitime » autorise une certaine souplesse aux responsables du traitement, cela ne signifie pas pour autant qu'elle est exempte de limites ou qu'elle peut être modelée pour satisfaire ou justifier toute opération de traitement. En effet, comme le rappelait la CNIL en décembre 2019, « L'intérêt légitime ne peut […] être considéré comme une base légale «par défaut» : il requiert au contraire un examen attentif de la part de l'organisme et le suivi d'une méthodologie rigoureuse ».[67] Pourtant cette base légale continue à être utilisée de manière abusive : une récente résolution du Parlement européen « s'inquiète de l'utilisation fréquente et abusive de l'intérêt légitime comme fondement juridique du traitement ».[68] Elle se poursuit ainsi :

> *Le Parlement européen [...] souligne que les responsables du traitement continuent de fonder leur action sur l'intérêt légitime sans procéder à la mise en balance des intérêts, qui comprend une évaluation des droits fondamentaux ; est particulièrement préoccupé par le fait que certains États membres adoptent des réglementations nationales pour déterminer les conditions du traitement fondées sur l'intérêt légitime, en prévoyant la mise en balance des intérêts respectifs du responsable du traitement et des personnes concernées, alors que le RGPD oblige chaque responsable du traitement à procéder individuellement à cette mise en balance et à se prévaloir de ce fondement juridique [...]*

L'évaluation des intérêts légitimes

71. Un responsable de traitement qui cherche à se fonder sur la base de l'intérêt légitime doit procéder à une évaluation et respecter une « obligation de transparence renforcée » en communiquant aux personnes concernées la « nature de l'intérêt légitime poursuivi » pour ces traitements.[69] Clearview n'a publié aucune évaluation d'intérêts légitimes en lien avec ses opérations de traitement. Dans sa correspondance avec Clearview, [redacted] a demandé à consulter une telle évaluation, mais n'a reçu aucune réponse (voir pièce 1).

---

[67] CNIL, « L'intérêt légitime : comment fonder un traitement sur cette base légale? », https://www.cnil.fr/fr/linteret-legitime-comment-fonder-un-traitement-sur-cette-base-legale.
[68] Résolution du Parlement européen du 25 mars 2021 sur le rapport d'évaluation de la Commission sur la mise en œuvre du règlement général sur la protection des données deux ans après son application (2020/2717(RSP)), paragraphe 7.
[69] CNIL, « L'intérêt légitime : comment fonder un traitement sur cette base légale? », https://www.cnil.fr/fr/linteret-legitime-comment-fonder-un-traitement-sur-cette-base-legale.

72. Une telle évaluation des intérêts légitimes doit être effectuée au regard des trois conditions énoncées à l'article 6, paragraphe 1, point f), et explicitées dans les arrêts *Rigas Satiksme*[70] et *Fashion ID*[71] de la CJUE :

(1) « **La poursuite d'un intérêt légitime par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées** » **(**« **finalité de traitement** »**)** – dans le cas de Clearview, il s'agirait d'un intérêt commercial, c'est-à-dire la fourniture d'un service à des tiers en échange d'une rémunération pécuniaire. Il va de soi que les entreprises ne sauraient considérer la seule poursuite de leurs modèles économiques ou du profit comme des « intérêts légitimes ». L'intérêt légitime des tiers auxquels les données sont divulguées peut être considéré comme l'identification d'individus dans le monde physique. Si l'on considère le type de client de Clearview le plus courant, à savoir un organisme chargé de l'application de la loi, l'article 6, paragraphe 1, du RGPD prévoit explicitement que la base légale des intérêts légitimes *« ne s'applique pas au traitement effectué par les autorités publiques dans l'exercice de leurs missions »*. S'agissant de tous les autres clients de Clearview, c'est-à-dire les entreprises privées et les particuliers, la légitimité de leur intérêt n'est que purement spéculative, et au mieux de nature limitée voire inquiétante. En tout état de cause, un intérêt futur et indéfini d'un tiers ne peut justifier les opérations de traitement initiales. En l'espèce, la collecte, le traitement biométrique et le stockage des images des personnes sont effectués avant que tout client n'utilise les données, et avant même que l'on puisse envisager l'usage spécifique qu'en feront les clients de Clearview. Comme l'a décrit le Commissariat à la protection de la vie privée du Canada, les activités de Clearview ne consistent en rien d'autre qu'en « l'identification et la surveillance de masse d'individus par une entité privée dans le cadre d'une activité commerciale ».[72]

(2) « **La nécessité du traitement des données à caractère personnel pour la réalisation de l'intérêt légitime poursuivi** » **(**« **nécessité** »**)** – si Clearview avait un intérêt légitime pertinent pour cette évaluation, cette condition exigerait d'évaluer si l'avantage commercial de la société pourrait être obtenu par des moyens moins intrusifs pour les droits et libertés fondamentaux des personnes concernées, conformément au principe selon lequel les dérogations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du strict nécessaire.[73] Après avoir établi que les intérêts d'une autorité répressive ne peuvent être pris en compte dans cette évaluation particulière, nul ne saurait soutenir qu'il est *nécessaire* pour les clients privés de Clearview d'utiliser l'outil dans leur intérêt. L'existence d'alternatives moins intrusives est cruciale, tout comme le principe de minimisation des données, selon

[70] Affaire 13/16 *Rigas Satiksme* [2017] ECLI:EU:C:2017:336, points 28 à 31.
[71] Affaire C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, point 95.
[72] CPVP (n 4), paragraphe 72.
[73] Affaires C-92/09 et C-93/09, *Volker und Markus Schecke et Eifert* [2010] EU:C:2010:662, point 86 ; affaire C-473/12 *IPI* [2013] EU:C:2013:715, point 39 ; affaire C-212/13 *Ryneš* [2014] EU:C:2014:2428, point 28.

lequel les données doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».[74] Par exemple, Clearview indique que les banques peuvent utiliser son outil afin d'effectuer des contrôles de sécurité et d'antécédents. Pourtant, les banques effectuent ces contrôles sans cet outil depuis des décennies. De plus, il est difficile de concevoir pourquoi de tels contrôles ne pourraient être effectués que sur la base d'une image faciale, plutôt que par le biais d'autres identifiants.

(3) « **Que les droits et les libertés fondamentaux de la personne concernée par la protection des données ne prévalent pas** » **(**« **mise en balance** »**)** – il s'agit de mettre en balance les intérêts du responsable du traitement et les effets du traitement sur la personne concernée. Dans l'affaire phare de *Google Spain*, la CJUE a considéré que :

> *un traitement de données à caractère personnel , tel que celui en cause au principal, réalisé par l'exploitant d'un moteur de recherche, est susceptible d'affecter significativement les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel lorsque la recherche à l'aide de ce moteur est effectuée à partir du nom d'une personne physique, dès lors que ledit traitement permet à tout internaute d'obtenir par la liste de résultats un aperçu structuré des informations relatives à cette personne trouvables sur Internet, qui touchent potentiellement à une multitude d'aspects de sa vie privée et qui, sans ledit moteur de recherche, n'auraient pas ou seulement que très difficilement pu être interconnectées, et ainsi d'établir un profil plus ou moins détaillé de celle-ci.*

La CJUE a également conclu que « [a]u vu de la gravité potentielle de cette ingérence, force est de constater que celle-ci ne saurait être justifiée par le seul intérêt économique de l'exploitant d'un tel moteur dans ce traitement. »[75]

Ce que la CJUE a décrit ici comme constituant une ingérence significative avec les droits fondamentaux des individus est précisément ce que fait Clearview, avec des facteurs qui ne peuvent que renforcer la gravité de cette ingérence : (a) utiliser l'outil conçu par Clearview, ne nécessite pas d'avoir le nom d'une personne pour obtenir des résultats de recherche, mais seulement son visage, qui peut être obtenu simplement en croisant une personne dans la rue et en la prenant en photo ; et (b) dans le cas de Clearview, une personne ne peut pas, sans utiliser elle-même le produit de la société, savoir quelles informations la concernant sont disponibles (alors qu'elle peut effectuer une recherche de son propre nom et d'autres identifiants textuels sur Google).

---

[74] C/Jorge Juan 6 28001 – Madrid, https://edpb.europa.eu/sites/edpb/files/article-60-final-decisions/es_2010_10_right_to_erasure_transparency_and_information_decisionpublic_redacted.pdf.
[75] Id., paragraphe 81.

L'avis du G29 portant sur la notion d'intérêt légitime[76] expose plus en détail certains des facteurs à prendre en considération lors de la réalisation d'une telle mise en balance :

i. **La nature et la source de l'intérêt légitime** – comme expliqué au paragraphe (1) ci-dessus, l'intérêt de Clearview dans le traitement est un intérêt purement commercial.

ii. **L'impact sur les personnes concernées**, y compris :

- la nature des données, par exemple si le traitement concerne des données qui peuvent être considérées comme sensibles ou si elles ont été obtenues à partir de sources accessibles au public – Clearview traite des données biométriques, qui sont des données particulièrement sensibles et, comme cela sera expliqué dans les paragraphes 88 et suivants ci-dessous, le fait que les données aient été obtenues à partir de sources accessibles au public n'enlève rien à leur caractère sensible et à la nécessité de protéger la vie privée. Le G29 a noté :

  > *il est important de souligner que les données à caractère personnel, même si elles ont été rendues publiques, continuent d'être considérées comme des données à caractère personnel, et leur traitement continue donc de nécessiter des garanties appropriées. L'article 7, point f), n'autorise pas de manière générale la réutilisation et le traitement ultérieur de données à caractère personnel accessibles au public.*[77]

  Tout en reconnaissant que le fait que les DACP soient accessibles au public peut être un facteur pertinent pour conclure à l'existence d'intérêts légitimes, le G29 a ensuite averti que ce ne serait le cas que « si la publication était effectuée dans l'attente raisonnable d'utilisation ultérieure des données à certaines fins (par exemple, à des fins de recherche ou à des fins liées à la transparence et à la responsabilité) »[78]. Comme expliqué ci-dessus dans la section C, le traitement effectué par Clearview ne peut en aucun cas s'inscrire dans le cadre de cette attente raisonnable d'utilisation ultérieure.

---

[76] Art 29 WP Avis sur les intérêts légitimes (n 64), pp. 36-43. **PI note que l'EDPB est en train de mettre à jour cet avis afin d'aborder les questions soulignées dans le rapport de la Commission adopté par la résolution du Parlement européen mentionnée ci-dessus (n 68), et que l'avis mis à jour ne peut qu'exiger une évaluation plus, et non moins, rigoureuse que celle présentée dans cette réclamation.**

[77] Id., p. 39 ; Traduit de l'anglais 'it is important to highlight that personal data, even if it has been made publicly available, continues to be considered as personal data, and its processing therefore continues to require appropriate safeguards. There is no blanket permission to reuse and further process publicly available personal data under Article 7(f).'

[78] Id. Traduit de l'anglais 'if the publication was carried out with a reasonable expectation of further use of the data for certain purposes (e.g. for purposes of research or for purposes related to transparency and accountability)'.

- la manière dont les données sont traitées (y compris si les données sont divulguées publiquement ou rendues accessibles à un grand nombre de personnes, ou si de grandes quantités de DACP sont traitées ou combinées avec d'autres données, par exemple en cas de profilage, à des fins commerciales, répressives ou autres) – les données traitées par Clearview sont soumises à l'algorithme de reconnaissance faciale de la société qui représente un type de traitement particulièrement intrusif. Tout client de Clearview peut accéder aux données traitées par l'entreprise. Il s'agit d'une population vaste, indéfinie et illimitée. En outre, l'assemblage de bribes d'informations sur la vie privée d'un individu, telles qu'elles ont été divulguées sur Internet de manière délibérée ou par inadvertance, peut conduire à la formation d'une vision très intrusive et intime de sa vie, qui n'aurait jamais pu être obtenue par une recherche manuelle en ligne ou l'utilisation de moteurs de recherche par mots clés. Sachant que ces renseignements peuvent être utilisés pour décider d'arrestations ou de condamnations pénales, l'impact sur les personnes concernées ne peut être décrit autrement que comme maximal.

- les attentes raisonnables des personnes concernées, notamment en ce qui concerne l'utilisation et la divulgation des données dans le contexte considéré – comme expliqué plus en détail dans la section C, les personnes concernées ne sauraient raisonnablement s'attendre à l'utilisation et la divulgation des données résultant du traitement de Clearview.

- le statut du responsable du traitement et de la personne concernée, y compris le rapport de force entre eux, ou le fait que la personne concernée soit un enfant ou appartienne à un groupe social vulnérable – les circonstances du traitement effectué par Clearview rendent l'impact sur les personnes concernées particulièrement sérieux. Comme l'indique clairement le considérant 47 du GDPR, ce qui est légitime doit reposer, au moins en partie, sur la question de savoir si un intérêt légitime est servi du fait de la relation entre le responsable du traitement et la personne concernée. Non seulement Clearview n'entretient aucune relation avec les personnes concernées, mais son existence et ses activités sont totalement inconnues de l'écrasante majorité d'entre elles. Si l'on ajoute à cela l'utilisation imprévisible de son outil par des autorités répressives et des entités privées du monde entier, ces circonstances rendent le rapport de force entre Clearview et les personnes concernées particulièrement défavorable à ces dernières. En outre, en raison de ses pratiques généralisées et indifférenciées, Clearview traite nécessairement des données personnelles d'enfants et de groupes sociaux vulnérables. Cette vulnérabilité est souvent amplifiée par le manque de contrôle de ces populations sur leurs identités en ligne.

L'avis du G29 sur les intérêts légitimes considère que dans les cas où il est particulièrement difficile d'anticiper ou d'établir un préjudice ou un dommage pour les personnes concernées :

> *il est d'autant plus important de privilégier la prévention et de veiller à ce que les activités de traitement des données ne puissent être réalisées que si elles ne comportent aucun risque ou un risque très faible de provoquer des conséquences négatives injustifiées pour les intérêts ou les libertés et droits fondamentaux des personnes concernées*[79].

Compte tenu de l'impact très important que le traitement de Clearview peut avoir sur les droits et libertés des personnes concernées, PI estime que la CNIL devrait adopter une approche particulièrement prudente et empêcher ce type de traitement particulièrement risqué.

iii. **L'existence de mesures compensatoires ou additionnelles en vue de limiter les impacts du traitement sur les personnes concernées**, notamment :

- minimisation des données – le modèle commercial de Clearview repose sur des principes opposés à la minimisation des données. En collectant et en traitant indistinctement les données par le biais de ses algorithmes de reconnaissance faciale, ce système s'apparente fortement à la collecte en masse d'ensembles de données et à de la surveillance de masse.

- mesures techniques et organisationnelles visant à interdire que les données servent à la prise de décision ou de mesures à l'endroit des personnes (« séparation fonctionnelle ») – la finalité ultime du produit Clearview est de permettre la prise de décisions et de mesures à l'égard des personnes, ce qui peut avoir un impact négatif important sur leur vie, comme expliqué plus en détail à la section VI-A ci-dessous.

- utilisation extensive de techniques d'anonymisation, agrégation de données, technologies d'amélioration de la confidentialité, respect du principe de la protection des données dès la conception, réalisation d'analyses d'impact relatives à la protection des données et à la vie privée – comme expliqué dans la section B ci-dessus, [redacted] n'a reçu aucune réponse à sa demande de copie d'une quelconque évaluation d'impact relative à la protection des données réalisée par Clearview. À notre connaissance, le produit de Clearview n'intègre aucune technologie ou modalité visant à

[79] Id., p.51, traduit de l'anglais : 'it is all the more important to focus on prevention and ensuring that data processing activities may only be carried out, provided they carry no risk or a very low risk of undue negative impact on the data subjects' interests or fundamental rights and freedoms'.

renforcer la protection de la vie privée. En tout état de cause, l'objectif même du produit Clearview est de priver toute personne ayant une quelconque empreinte numérique (intentionnelle ou non) de la protection de son identité à laquelle elle peut raisonnablement s'attendre.

- une transparence renforcée, un droit d'opposition inconditionnel, l'existence de mesures connexes visant à responsabiliser les personnes concernées. Ces questions jouent « un rôle crucial dans le contexte de l'article 7, point f)[80] et exigent du responsable du traitement qu'il « effectue au préalable une évaluation attentive, fondée sur des faits spécifiques plutôt que de manière abstraite, en tenant également compte des attentes raisonnables des personnes concernées »[81]. A la connaissance de PI, Cleaview n'a jamais effectué ou montré qu'elle effectuait le test de mise en balance entre les droits et intérêts en cause, et ce, en dépit de multiples occasions de le faire telles que dans sa politique de confidentialité, ou lors du traitement des multiples demandes de droit d'accès que l'entreprise reçoit. Comme expliqué ci-dessus dans la section B, les activités de Clearview témoignent d'un manque total de transparence et de responsabilité envers les personnes concernées. Clearview a au préalable offert un droit limité de s'opposer au traitement (exerçable par les formulaires mentionnés au paragraphe 26 ci-dessus) mais la portée de l'exercice de ce droit est loin d'être claire. En raison de la nature de la technologie de Clearview, il est probable que toute possibilité d'opposition au traitement n'affecterait en réalité que le retour des résultats lorsqu'une recherche est effectuée, et ne limiterait ni la collecte ultérieure de DACP, ni le traitement ultérieur effectué par le biais des algorithmes de reconnaissance faciale de la société.

73. Se fondant sur le cadre ci-dessus pour analyser l'applicabilité de la base légale de l'intérêt légitime aux opérations de traitement de Clearview, il est clair qu'en l'espèce, sur chaque critère à prendre en compte, le responsable du traitement tombe dans la catégorie des risques élevés et des impacts négatifs élevés. En outre, les diverses mesures « compensatoires » à la portée de l'entreprise et qui permettraient de limiter les impacts du traitement sont tout simplement absentes de ses activités. Comme tout intérêt légitime est ici au mieux un intérêt commercial, la « balance » penche contre la conformité du traitement et la validité de toute base légale en application de l'article 6, paragraphe 1, point f).

74. Des évaluations des intérêts légitimes ont été conduites par certaines autorités de protection des données européennes et témoignent d'une interprétation très restrictive qui ne saurait en aucun cas s'étendre au type de traitement

[80] Id., p.43.
[81] Id., p.43, traduit de l'anglais 'perform a careful and effective test in advance, based on the specific facts of the case rather than in an abstract manner, taking also into account the reasonable expectations of data subjects'.

généralisé et indifférencié qu'opère Clearview. Par exemple, dans sa décision n° 35/2020,[82] la Chambre Contentieuse de l'Autorité de Protection des Données belge a évalué si la réutilisation de la photo de profil Facebook librement accessible au public d'un individu par une autorité judiciaire belge pour faire appliquer une interdiction de fréquentation relevait des intérêts légitimes de l'autorité. Elle a noté :

> *Le RGPD comporte une limitation considérable de la possibilité de réutilisation de données à caractère personnel qui peuvent être consultées publiquement. La Chambre Contentieuse souligne ainsi que le principe en vigueur est le suivant : le fait qu'une photo de profil d'une personne soit librement accessible au public ne signifie pas que d'autres puissent l'utiliser librement. L'utilisation de cette photo n'est possible que si une base juridique existe à cet effet.*

La Chambre Contentieuse a décidé que la réutilisation de la photo de l'intéressé relevait bien de la base légale de l'intérêt légitime, car l'autorité avait un intérêt légitime (l'exécution de sa décision), pour la réalisation duquel le traitement était nécessaire (il ne pouvait être réalisé par aucun autre moyen, et l'autorité a pris soin de brouiller les visages des autres personnes figurant sur la photo). Cette base légale était spécifique à la plainte individuelle et ne pouvait pas être étendue de manière indifférenciée. Le soin apporté par l'Autorité de Protection des Données belge à autoriser la réutilisation spécifique et limitée de la photo de profil du plaignant démontre le caractère totalement disproportionné et inacceptable d'autoriser la collecte et la réutilisation généralisée et indifférenciée par Clearview de chaque image faciale disponible sur Internet.

75. De même, le Commissariat à la protection de la vie privée du Canada a procédé à l'équivalent d'une évaluation des intérêts légitimes dans son champ de compétence et a conclu :

> *À notre avis, dans les circonstances, Clearview ne peut justifier aucune fin acceptable en ce qui a trait aux aspects suivants :*
>
> *i. le prélèvement massif et systématique des images de millions d'individus partout au Canada, y compris des enfants, parmi plus de 3 milliards d'images qui ont été prélevées dans le monde entier ;*
>
> *ii. l'élaboration d'un dispositif biométrique de reconnaissance faciale reposant sur ces images et la conservation de ces renseignements même après que l'image d'origine ou le lien ait été retiré d'Internet ; ou*
>
> *iii. l'utilisation et la communication ultérieures de ces renseignements à ses propres fins commerciales ;*
>
> *lorsque ces fins :*

[82] Autorité de Protection des Données, Chambre Contentieuse, Décision quant au fond 35/2020 du 30 juin 2020 (Numéro de dossier : DOS-2019-01240), https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-35-2020.pdf.

iv. *sont sans rapport avec les fins pour lesquelles les images ont été publiées à l'origine (p. ex. médias sociaux ou réseautage professionnel) ;*
v. *sont souvent au détriment de la personne (enquête, poursuites éventuelles, embarras, etc.) ;*
vi. *présentent un risque de préjudice grave aux individus dont les images sont recueillies par Clearview (y compris les préjudices associés à une erreur d'identification ou à d'éventuelles atteintes à la sécurité des données), alors que la grande majorité des individus en question n'ont jamais été impliqués dans un crime et ne le seront jamais plus qu'ils seront désignés pour contribuer à la résolution d'un crime grave.*

76. Pour compléter et préciser l'évaluation ci-dessus de l'impact sur les personnes concernées, les sections suivantes mettent en évidence trois aspects essentiels du préjudice causé aux personnes concernées par l'outil de Clearview : (a) les risques reconnus du traitement de données biométriques, (b) l'effet dissuasif inévitable dans l'exercice de certains droits fondamentaux, et (c) les préjudices particuliers à envisager pour les personnes vulnérables.

(a) Risques liés au traitement de données biométriques

77. Les données biométriques sont considérées comme des catégories particulières de données car il s'agit de données uniques, générées à partir de caractéristiques humaines, telles que les empreintes digitales, la voix, le visage, la rétine et l'iris, la géométrie de la main, la démarche ou les profils génétiques. Il s'agit en soi de données sensibles, quelle que soit leur origine ou leur mode de collecte.[83] Comme le constate le Commissariat à la protection de la vie privée du Canada :

> *Les renseignements biométriques sont distinctifs, peu susceptibles de varier dans le temps, difficiles à modifier et en grande partie propres à la personne. Les données biométriques faciales sont de nature particulièrement sensible, car elles constituent l'essence de l'identité d'une personne et permettent d'identifier et de surveiller les personnes.*[84]

78. Lorsqu'elles sont adoptées en l'absence de cadres juridiques robustes et de garanties strictes, les technologies biométriques constituent de graves menaces pour la vie privée et la sécurité des personnes, car leur application peut être élargie afin de faciliter la discrimination, le profilage et la surveillance de masse.[85] En l'état actuel des choses, avec un outil comme celui de Clearview, l'empreinte faciale d'une personne peut être utilisée pour trouver son nom et ses comptes sur les réseaux sociaux, et pour combiner ces informations avec sa présence physique dans la rue, les magasins qu'elle fréquente et les photos qu'elle ou ses amis publient en ligne – une extension massive des modes d'utilisation, pour l'essentiel limités, de la biométrie jusqu'à

[83] *S. et Marper c. Royaume-Uni* [GC], App nos 30562/04 et 30566/0 (CEDH, 12 avril 2008).
[84] CPVP (n. 4), paragraphe 74.
[85] Privacy International, 'Biometrics', https://privacyinternational.org/learn/biometrics.

présent. Selon le Haut-Commissaire des Nations Unies aux droits de l'homme, « [e]nregistrer, analyser et conserver les images faciales d'un individu sans son consentement revient à s'ingérer dans l'exercice de son droit à la vie privée. »[86]

79. Comme il est intrinsèquement difficile, voire impossible, de les modifier, les données biométriques permettent d'identifier une personne pendant toute sa vie. Cela rend la création de bases de données biométriques problématique, car les risques doivent être anticipés à long terme, qu'il s'agisse d'un changement de situation politique ou de régime, d'une future violation de DACP ou du développement de technologies permettant d'utiliser les données biométriques à de nouvelles fins et de révéler plus d'informations sur les personnes que ce qui est actuellement possible. Aussi, la collecte et le stockage de données biométriques peuvent faire l'objet de graves abus.[87]

80. Le G29 reconnaissait déjà il y a quelques années l'importance du traitement des données biométriques : « Les données biométriques changent de manière irrévocable la relation entre le corps et l'identité car elles rendent les caractéristiques physiques «lisibles par une machine» et sujettes à une utilisation ultérieure ».[88] Il prédisait déjà les préjudices qui seraient soulevés par l'extraction de caractéristiques biométriques à partir d'informations accessibles au public, et a précisément anticipé les opérations de traitement de Clearview :

> *Les photographies sur Internet, sur des réseaux sociaux et dans des applications de gestion ou de partage de photos en ligne ne peuvent être traitées ultérieurement afin d'extraire des modèles biométriques ou de les inscrire dans un système biométrique pour reconnaître automatiquement les personnes sur les photos (reconnaissance faciale) sans base juridique spécifique (par ex., consentement) pour cette nouvelle finalité. Si cette finalité secondaire a une base juridique, le traitement doit également être adéquat, pertinent et non excessif au regard de cette finalité.*[89]

81. Les dommages causés par les traitements de données biométriques sont encore plus importants et préoccupants pour les droits fondamentaux lorsqu'ils résultent de l'usage des forces de l'ordre. Nous les examinons plus en détail dans la section VI.A ci-dessous. En tout état de cause, PI soutient que les risques engendrés par un traitement généralisé et indifférencié de données biométriques sont trop importants pour qu'une entité privée soit autorisée à effectuer un tel traitement.

(b) Effet dissuasif sur l'exercice des droits fondamentaux

---

[86] Haut-Commissaire des Nations unies aux droits de l'homme (HCHD), « Incidence des nouvelles technologies sur la promotion et la protection des droits de l'homme dans le contexte des rassemblements, y compris des manifestations pacifiques » (Doc.A/HRC/44/24, 24 juin 2020), https://undocs.org/fr/A/HRC/44/24.
[87] Voir le rapport du HCDH, « Le droit à la vie privée à l'ère numérique » (Doc.A/HRC/39/29, 3 août 2018). https://undocs.org/A/HRC/39/29.
[88] Groupe de travail Article 29 sur la protection des données, « Avis 03/2012 sur l'évolution des technologies biométriques », https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp193_fr.pdf.
[89] Id.

82. Le G29 prévoit que lors de l'évaluation de l'impact du traitement, « [l]'effet dissuasif sur l'exercice des droits fondamentaux, tels que la liberté de la recherche ou la liberté d'expression, pouvant résulter d'une surveillance ou d'un suivi continu, doit également être suffisamment pris en considération ».[90] PI souhaite attirer l'attention sur la jurisprudence des tribunaux et des autorités allemandes, qui ont procédé à des évaluations approfondies de l'impact de la vidéosurveillance sur les droits fondamentaux dans le cadre d'évaluations d'intérêts légitimes. En effet, l'autorité de protection des données du Bade-Wurtemberg a souligné l'importance de prendre en compte le droit de l'individu au libre développement de sa personnalité lors de l'évaluation de l'intensité des contrôles par vidéosurveillance[91]. Pour cette autorité, dans les restaurants, les parcs d'attraction et, d'une manière générale, les lieux où les gens se rassemblent pour manger, boire, discuter et se détendre, le droit au libre épanouissement de la personnalité doit l'emporter sur les intérêts légitimes du responsable du traitement. Internet étant devenu un lieu de socialisation au même titre que ces espaces publics, le même principe devrait s'y appliquer. En outre, les risques de la vidéosurveillance identifiés sont aggravés lorsque l'identification massive dans le monde physique est permise par la technologie de Clearview.

83. Le CEPD a explicitement reconnu que la *social media intelligence* (SOCMINT), méthode de recherche d'informations en sources ouvertes correspondant précisément à ce que la technologie de Clearview permet et a été conçue pour faciliter, a des effets dissuasifs importants sur l'exercice de divers droits et libertés fondamentaux :

> *La surveillance des utilisateurs des réseaux sociaux est une opération de traitement de données à caractère personnel qui crée un risque élevé pour les droits et libertés des personnes. La réutilisation des données est susceptible d'affecter l'autodétermination de l'information d'une personne et de réduire encore le contrôle des personnes concernées sur leurs données... En effet, la diminution de l'espace intime disponible pour les personnes, du fait de la surveillance inévitable par les entreprises et les gouvernements, a un effet dissuasif sur la capacité et la volonté des personnes de s'exprimer et de nouer des relations librement, y compris dans la sphère civique si essentielle à la vie démocratique.*[92]

---

[90] Opinion du G29 sur les intérêts légitimes (n 76), traduit de l'anglais '[t]he chilling effect on protected behaviour, such as freedom of research or free speech, that may result from continuous monitoring/tracking, must also be given due consideration.'

[91] Der Landesbeauftragte für den Datenschutz Baden-Württemberg, Orientierungshilfe 'Videoüberwachung durch nicht-öffentliche Stellen', p. 9.

[92] CEPD (n 57). Traduit de l'anglais : 'Social media users monitoring is a personal data processing activity that creates high risk for individuals' rights and freedoms. Repurposing of data is likely to affect a person's information self-determination, further reduce the control of data subjects over their data... Indeed, the diminution of intimate space available to people, as a result of unavoidable surveillance by companies and governments, has a chilling effect on people's ability and willingness to express themselves and form relationships freely, including in the civic sphere so essential to the health of democracy.'

84. En outre, le Comité des droits de l'homme des Nations Unies a recommandé de faire preuve de prudence s'agissant des pratiques de *social media intelligence*. L'Observation générale no 37 (2020) sur le droit de réunion pacifique (art. 21) du Pacte international relatif aux droits civils et politiques a établi que :

> *Le fait qu'une réunion se tienne en public n'empêche pas que des atteintes à la vie privée des participants puissent être commises. [...] Il en va de même en ce qui concerne la surveillance des médias sociaux visant à glaner des informations sur les participants à des réunions pacifiques. Les décisions visant la collecte d'informations et de données personnelles sur les participants à des rassemblements pacifiques et celles concernant le partage ou la conservation de ces informations et données doivent faire l'objet d'un contrôle indépendant et transparent.*[93]

85. Internet et les plateformes de réseaux sociaux ont acquis un rôle essentiel dans le développement de la vie privée, sociale et politique des individus, ainsi que de leur identité en ligne. Ils définissent le contexte numérique des espaces civiques d'aujourd'hui, où les gens accèdent à l'information, formulent et discutent des idées, soulèvent des opinions divergentes, réfléchissent à des réformes possibles, dénoncent les préjugés et la corruption, et s'organisent pour plaider en faveur de changements politiques, économiques, sociaux, environnementaux et culturels.[94]

86. Pour faire d'Internet un espace sain, dynamique et ouvert, il est essentiel que les individus s'y sentent libres de partager des informations personnelles et des photos comme ils l'entendent, sans craindre que ces données ne soient immédiatement saisies et stockées à des fins dissimulées. Or, la liberté de se définir soi-même comme on l'entend sur Internet, en contrôlant la diffusion de différents éléments d'information à différents endroits est en passe de disparaître sous la menace imminente de voir toutes ces informations traçables et unifiées en un simple clic.

(c) Préjudices pour les groupes de personnes vulnérables

87. L'outil de Clearview peut également causer un préjudice particulier aux personnes en situation vulnérable. Pour cette section, nous avons été largement inspirés par le travail de l'Union américaine pour les libertés civiles (ACLU), et nous souhaitons attirer l'attention sur ce travail, dans le cadre de la plainte que l'organisation a déposée à l'encontre de Clearview dans l'État de l'Illinois en vertu de la loi BIPA.[95]

---

[93] Disponible sur https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx.
[94] Privacy International, 'Protecting civic spaces' (mai 2019), https://privacyinternational.org/sites/default/files/2019-07/Protectin%20civic%20spaces%20PI%20May%202019.pdf.
[95] Plainte, ACLU et autres contre Clearview AI, Inc, Circuit Court of Cook County, Illinois, Case No. : 2020 CH 04353, https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint.

88. Les personnes en situation vulnérable courent un risque accru s'ils sont identifiés alors qu'ils vaquent à leurs occupations quotidiennes. Les survivants de violences sexuelles ou d'exploitation sexuelle à des fins commerciales, par exemple, ou les migrants, ont été à maintes reprises la cible de harcèlement ou de discrimination de la part de particuliers comme de policiers. « En privant ces personnes du contrôle et de la sécurité de leurs identifiants biométriques sensibles et en menaçant de rendre trivialement facile leur identification et leur suivi en ligne et dans le monde physique, le système Clearview les expose à la traque, au harcèlement et à la violence. »[96] La crainte d'être identifiées peut également amener ces personnes à éviter de se rendre dans des lieux et des réunions où elles pourraient bénéficier de l'assistance et de la protection dont elles ont besoin.

89. En outre, le hachage des vecteurs effectué lorsque Clearview extrait les caractéristiques biométriques des images faciales permet potentiellement de catégoriser les visages des personnes en fonction de leur degré de similitude. Les clients de Clearview pourraient ainsi procéder à des regroupements automatiques de personnes en fonction de leur origine ethnique, de leur couleur de peau ou de toute autre catégorisation, ce qui ouvrirait la voie à un suivi et une surveillance discriminatoires, ou à des pratiques telles que la police prédictive.

90. Après avoir exposé les risques et préjudices multiples et graves que les activités de Clearview font peser sur les droits et libertés fondamentaux des personnes, PI soutient que l'évaluation de la « mise en balance » des droits et intérêts en cause doit aller à l'encontre de toute constatation d'une base légale valable au titre de l'article 6, paragraphe 1, point f), du RGPD. Cette absence de base légale en vertu de l'article 6 du RGPD est suffisante pour conclure à un traitement illégal. Toutefois, dans l'éventualité où la CNIL ne partagerait pas ce point de vue, la section suivante se propose d'analyser l'applicabilité d'une base légale s'agissant des traitements de catégories particulières de DACP.

<u>Manifestement rendues publiques – Article 9, paragraphe 2, point e) du RGPD</u>

91. Dans la mesure où Clearview traite des catégories particulières de DACP, en plus d'une base légale valide en application de l'article 6 (qui est absente en l'espèce, comme l'a démontré la section précédente), le responsable du traitement doit également satisfaire au moins une des conditions de l'article 9 paragraphe 2. Dans le cas de Clearview, la seule condition pertinente est que « le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée », conformément à l'article 9, paragraphe 2, point e), du RGPD. PI note que même si cette condition était applicable, elle ne s'appliquerait qu'aux images faciales que

[96] Réponse du plaignant à la motion de rejet du défendeur, ACLU et autres contre Clearview AI, Inc, Circuit Court of Cook County, Illinois, affaire n° 2020 CH 04353, traduit de l'anglais 'By divesting these individuals of control over and security in their sensitive biometric identifiers and threatening to make it trivially easy to identify and track them both online and in the physical world, Clearview's system exposes them to stalking, harassment, and violence.'

Clearview collecte en ligne (données biométriques en tant que telles, voir en ce sens la section V.A ci-dessus). Les données biométriques que Clearview crée par extraction vectorielle ne peuvent en aucun cas remplir cette condition.

92. Le fait que les informations soient accessibles au public en ligne ne permet pas d'établir automatiquement une base légale de traitement au titre de l'article 9. Comme le reconnaissent à juste titre les différentes recommandations des autorités de protection des données et les publications scientifiques associées à celles-ci,[97] l'exception prévue à l'article 9, paragraphe 2, point e), doit être interprétée de manière restrictive. En particulier, les termes « manifestement » et « par la personne concernée » exigent des circonstances très spécifiques dans lesquelles les DACP ont été rendues publiques.

93. Premièrement, les informations accessibles au public en ligne doivent continuer à bénéficier d'un degré élevé de protection de la vie privée. Cela est crucial pour faire d'Internet un espace sain et ouvert où les individus peuvent librement exercer leurs droits et libertés fondamentaux. L'outil de reconnaissance faciale de Clearview est l'archétype d'une nouvelle technologie à première vue inoffensive qui, si elle est autorisée à être déployée et utilisée à grande échelle, pourrait modifier profondément Internet tel que nous le connaissons, ainsi que le comportement des individus en ligne. Cette technologie repose sur l'hypothèse erronée selon laquelle ce qui est accessible au public sur Internet appartient immédiatement à une sphère entièrement publique et a été offert gracieusement au monde entier, lequel peut voir instantanément et réutiliser ces données à volonté. Or, le clivage entre sphère publique et sphère privée n'est guère pertinent dans une société moderne où une grande partie de notre vie économique, sociale et démocratique se déroule en ligne. C'est mal comprendre Internet que de considérer cet espace comme un forum homogène, entièrement public et totalement accessible, sur lequel chacun consent à ce que ses informations personnelles soient librement accessibles à tous dès qu'elles se trouvent dans une partie techniquement publique de ce dernier.[98]

94. Les dangers d'un tel clivage sont également très concrets dans le monde physique, comme l'a déjà reconnu la Cour européenne des droits de l'homme. Dans l'affaire *Peck c. Royaume-Uni*[99], la Cour a jugé que la divulgation aux médias, à des fins de diffusion, de séquences vidéo du requérant dont la tentative de suicide avait été filmée par des caméras de vidéosurveillance a constitué une ingérence grave dans la vie privée du requérant, bien qu'il se soit trouvé dans un lieu public à ce moment-là. Le raisonnement de la CEDH s'est fondé sur l'hypothèse qu'aucune personne ne pouvait raisonnablement s'attendre à ce que des séquences décrivant des aspects sensibles de sa vie

[97] Pour plus d'informations et des références aux recommandations des autorités de protection des données, voir Edward S Dove et Jiahong Chen, 'What does it mean for a data subject to make their personal data 'manifestly public' ? An analysis of RGPD Article 9(2)(e)' (2021) Vol. 00, No. 0, International Data Privacy Law, 1, 2, https://doi.org/10.1093/idpl/ipab005.

[98] Voir la citation du CEPD citée au paragraphe 83 ci-dessus, ainsi que la citation du CDH citée au paragraphe 84.

[99] App no 44647/98 (CEDH, 28 janvier 2003), paragraphes 53, 61-62.

privée soient ultérieurement diffusées dans les médias, même si ses actes sont « à la disposition du grand public ». [100]

95. Deuxièmement, il est de notoriété publique pour toute personne même vaguement initiée à l'utilisation d'Internet et des réseaux sociaux, que de nombreuses photos de personnes accessibles en ligne n'ont pas été rendues publiques *par la personne concernée* elle-même. Les réseaux sociaux permettent à leurs utilisateurs de téléverser des photos d'eux-mêmes et de toute autre personne. Ces dernières (qu'il s'agisse d'amis du « téléverseur », de passants inconnus dans des espaces publics, ou de clients de commerces qui publient des photos de leur établissement et de leurs clients sans l'aval de ces derniers) n'ont pas elles-mêmes mis en ligne leurs images faciales et peuvent même ignorer que des photos contenant leur visage ont été téléversées et sont disponibles publiquement en ligne.

96. Le Commissariat à la vie privée du Canada est parvenu à la même conclusion lorsqu'il s'est agi de déterminer si les données personnelles collectées par Clearview relevaient de l'exception canadienne relative aux *« publications »*, qui ne s'applique que « si l'intéressé a fourni les renseignements » ou lorsqu' « il est raisonnable de supposer que la personne sur laquelle portent les renseignements a fourni ces renseignements ». Pour l'autorité canadienne, « [c]omme Clearview réalise une collecte massive d'images, au moyen d'outils automatisés, il est inévitable que dans de nombreux cas, les images aient été téléchargées par une tierce partie ».[101]

97. Troisièmement, comme expliqué dans la section III, une fois collectées, les photos sont conservées indéfiniment dans la base de données de Clearview, sans se soucier de savoir si ces photos sont encore accessibles au public à un quelconque moment. Comme le fait remarquer à juste titre un article du New York Times sur Clearview, « si votre profil a déjà été *scraped*, il est trop tard. La société conserve toutes les images qu'elle a extraites, même si elles ont été supprimées ou retirées par la suite ».[102] L'article poursuit en indiquant que « M. Ton-That a toutefois déclaré que la société travaillait sur un outil qui permettrait aux personnes de demander le retrait des images si elles ont été retirées de leur site internet d'origine ». S'agissant de cette dernière « excuse », il est tout d'abord inacceptable que Clearview ait déployé sa technologie sans l'existence de cet outil. En outre, un tel outil ne fournirait de toute façon qu'une possibilité de recours extrêmement limitée pour les individus. Cet outil impliquerait que les personnes (1) sachent en premier lieu que Clearview collecte leurs images faciales, (2) introduisent systématiquement des demandes de droit d'accès afin de savoir quelles photos ont été collectées par Clearview, (3) croisent les résultats de ces demandes avec ce qu'elles ont mis en ligne, et (4) soumettent

[100] Id.
[101] CPVP (n 4), paragraphe 66.
[102] Hill (n 6), traduit de l'anglais 'if your profile has already been scraped, it is too late. The company keeps all the images it has scraped even if they are later deleted or taken down' ; Id., traduit de l'anglais : 'though Mr. Ton-That said the company was working on a tool that would let people request that images be removed if they had been taken down from the website of origin.'

des demandes individuelles de retrait. Cette approche est totalement insensée et constitue un affront flagrant au droit à contrôler son identité en ligne, empêchant tout exercice effectif des droits des personnes concernées prévus par le RGPD.

98. Enfin, de façon générale les paramètres de confidentialité des plateformes sont réputés pour être difficiles à mettre en place et à ajuster de manière à ce que les informations que l'on souhaite voir rester dans des cercles privés en ligne le soient effectivement et le restent. Les recherches menées par PI ont montré à plusieurs reprises à quel point il est complexe pour les individus d'ajuster leurs paramètres afin de respecter la vie privée, et que les exigences légales en matière de consentement ne sont souvent pas respectées.[103] Le terme anglophone de « dark patterns » signifie que les personnes concernées n'ont pas toujours le contrôle de leurs données personnelles en ligne. [104]La CNIL observe d'ailleurs dans son rapport *La forme des choix* qu'à travers des pratiques de « design abusif », « design trompeur » ou « design dangereux », « les individus sont confrontés à des biais qui peuvent être autant d'instruments, ce qu'ont bien compris certains acteurs et qui peut avoir des impacts significatifs du point de vue de la protection des données ». [105]

99. PI estime donc que Clearview ne peut remplir aucune condition pour le traitement de catégories particulières de données en application de l'article 9, paragraphe 2, point e), du RGPD.

E. Finalité du traitement

100. Un autre principe essentiel de la protection des données ouvertement bafoué par le traitement effectué par Clearview est celui de la « limitation des finalités » prévu à l'article 5, paragraphe 1, point b), du RGPD. L'application de ce principe doit tenir compte des facteurs énumérés à l'article 6, paragraphe 4, qui, en l'espèce, indiquent clairement que le traitement effectué par Clearview n'est pas compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement diffusées.

101. La question de la finalité du traitement est intrinsèquement liée aux attentes légitimes des personnes quant à l'utilisation de leurs données personnelles accessibles au public (voir en ce sens les paragraphes 54à 64 ci-dessus). En effet, chaque acte de publication de données est effectué pour une finalité définie. La publication d'un CV sur un site personnel est effectuée aux fins de trouver un emploi – un responsable de traitement mépriserait clairement cette

[103] Privacy International, 'Most cookie banners are annoying and deceptive. This is not consent.' (21 mai 2019), https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent. Privacy International, 'Facebook – Profile Settings' (7 janvier 2021), https://privacyinternational.org/guide-step/3959/facebook-profile-settings.
[104] Conseil norvégien des consommateurs, 'Deceived by Design - How tech companies use dark patterns to discourage us from exercising our rights to privacy' (27 juin 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.
[105] CNIL, « La forme des choix - Données personnelles, design et frictions désirables », Cahiers IP, N°06 (Janvier 2019), p. 27, https://www.cnil.fr/sites/default/files/atoms/files/cnil_cahiers_ip6.pdf.

finalité s'il venait à utiliser les données contenues dans ce CV à des fins publicitaires.

102. PI a démontré que la réutilisation de ces données aux fins d'effectuer un traitement dans une base de données biométriques excède de toute évidence ces attentes. Comme l'indique le CEPD, l'exploitation de DACP dans le cadre de pratiques telles que la *social media intelligence* « entraîne souvent une utilisation des données à caractère personnel au-delà de leur finalité initiale, de leur contexte initial et d'une manière que la personne ne pouvait raisonnablement pas anticiper. »[106]

103. L'extrait suivant de l'avis du G29 sur l'évolution des données biométriques est également révélateur :

> *Les photographies sur l'internet, sur des réseaux sociaux et dans des applications de gestion ou de partage de photos en ligne ne peuvent être traitées ultérieurement afin d'extraire des modèles biométriques ou de les inscrire dans un système biométrique pour reconnaître automatiquement les personnes sur les photos (reconnaissance faciale) sans base juridique spécifique (par ex., consentement) pour cette nouvelle finalité. Si cette finalité secondaire a une base juridique, le traitement doit également être adéquat, pertinent et non excessif au regard de cette finalité. Si le sujet a accepté que les photographies où il apparaît puissent être traitées pour l'étiqueter automatiquement dans un album de photos en ligne par un algorithme de reconnaissance faciale, ce traitement doit être réalisé dans le respect de la protection des données : les données biométriques qui ne sont plus nécessaires après l'étiquetage des photographies avec le nom, le surnom ou tout autre texte spécifié par le sujet doivent être supprimées. La création d'une base de données biométriques permanente n'est a priori pas nécessaire à cette fin.*[107]

104. À la lumière de cette citation, le traitement effectué par Clearview constitue une finalité entièrement nouvelle par rapport à la publication originale, finalité pour laquelle la société devrait se fonder sur une base légale distincte et valide. Or, comme nous l'avons démontré dans la section V.D ci-dessus, celle-ci est inexistante. Clearview viole donc le principe de la finalité du traitement.

105. PI conclut que les pratiques de Clearview constituent des violations des principes de transparence, de loyauté et de limitation des finalités, ainsi que de l'exigence de fonder tout traitement de DACP sur une base légale. PI ne cherchera pas à évaluer la conformité au RGPD de l'utilisation de l'outil par les clients de Clearview autre que celle des forces de l'ordre, car ce sont les seuls clients auxquels Clearview s'adresse aujourd'hui ouvertement. Nous souhaitons cependant attirer l'attention de la CNIL sur les prévisions rapportées

[106] CEPD (n 57). Traduit de l'anglais : 'often result in personal data being used beyond their initial purpose, their initial context and in ways the individual could not reasonably anticipate'.
[107] Art 29 WP (n 82), p.7.

par « des officiers de police et des investisseurs de Clearview » selon lesquelles l'outil « sera à terme disponible pour le public ».[108]

VI. Cadre juridique et préoccupations : Traitement par les autorités répressives (directive Police-Justice)

106. Toute limitation des droits fondamentaux des personnes doit être effectuée au-travers de mesures législatives sur des questions aussi importantes que la sécurité nationale, la défense nationale, la prévention, la recherche, la prévention, détection ou la poursuite d'infractions pénales, etc.[109] Si de telles limitations peuvent s'appliquer aux opérations de traitement menées par les autorités répressives comme le prévoit la directive Police-Justice, elles ne sauraient en aucun cas s'appliquer à une entreprise privée collectant sans discernement des DACP dans le but potentiel ultime de vendre l'utilisation de sa base de données à des autorités strictement réglementées. Comme PI l'a observé à plusieurs reprises dans le cadre de ses travaux,[110] l'utilisation d'outils privés à des fins policières conduit souvent à contourner les garanties exigeantes imposées aux autorités publiques en matière de droits fondamentaux.

107. Quand bien même PI considère que les violations du RGPD identifiées dans la section V sont suffisantes en tant que telles pour justifier du prononcé de mesures correctrices suite à la collecte de DACP des personnes concernées opérée par Clearview, ces violations deviennent d'autant plus graves lorsqu'elles sont analysées en lien avec l'utilisation finale envisagée de ces DACP. Dans l'hypothèse où la CNIL serait disposée à autoriser les pratiques de collecte de Clearview dans l'UE, PI soutient que pour limiter le préjudice causé aux personnes concernées, l'utilisation de ces DACP par les autorités répressives devrait être interdite. Celle-ci suscite en effet de graves préoccupations et contrevient aux dispositions de la directive Police-Justice.

108. Cette partie de la réclamation se propose d'exposer dans un premier temps les inquiétudes de PI concernant l'utilisation potentielle par les forces de l'ordre de technologies de reconnaissance faciale ainsi que de techniques de renseignement sur les réseaux sociaux (dites SOCMINT ou *social media intelligence*). Nous sommes particulièrement inquiets des situations où ces technologies font l'objet d'une utilisation couplée, comme dans le cas de Clearview. Ces inquiétudes se traduisent en pratique par diverses violations de la directive Police-Justice que nous examinerons dans un second temps, en particulier s'agissant des exigences de licéité et de nécessité visées aux articles 87 et 88 de la LIL.

---

[108] Hill (n 6).
[109] Article 23 du RGPD
[110] Voir par exemple : Privacy International, 'Public-Private surveillance partnerships', https://privacyinternational.org/campaigns/unmasking-policing-inc ; Privacy International, 'One Ring to watch them all' (25 juin 2020). https://privacyinternational.org/long-read/3971/one-ring-watch-them-all.

A. Inquiétudes quant à l'utilisation par la police de technologies de reconnaissance faciale et de SOCMINT

109. L'utilisation de technologies de reconnaissance faciale par les forces de police a un impact profond sur la manière dont notre société est surveillée et contrôlée. Le déploiement d'une technologie aussi intrusive pose non seulement des questions importantes en matière de protection de la vie privée et des données, mais aussi des questions éthiques quant à l'opportunité pour les démocraties modernes d'autoriser son utilisation. Avec l'outil de Clearview en main, la police peut effectivement identifier chaque personne filmée (ou du moins associer son identité physique à sa présence en ligne). Il est tout à fait réaliste de penser qu'un service de police pourrait décider d'identifier chaque individu dans une foule de manifestants et d'établir des profils sur eux à partir d'informations collectées en ligne. Cette perspective parfaitement dystopique trouve un prolongement des plus réalistes dans l'outil de Clearview.

110. Dans sa contribution au débat national français portant sur la reconnaissance faciale, la CNIL a souligné :

> *(…) à la différence par exemple des systèmes de captation et de traitement vidéo, qui nécessitent la mise en place de dispositifs physiques, la reconnaissance faciale est une fonctionnalité logicielle qui peut être mise en œuvre au sein de systèmes existants (caméras, base de données de photos, etc.). Cette fonctionnalité peut donc être connectée, branchée sur une multitude de systèmes, et combinée avec d'autres fonctionnalités.*
>
> *Le débat autour de la reconnaissance faciale doit tenir compte de ce continuum technologique. Il s'agit de ne pas plaquer sur des besoins opérationnels précis des technologies inutilement intrusives, alors que des techniques ou des mesures ayant un moindre impact seraient tout autant, voire plus efficaces. Mais il faut aussi intégrer dans l'équation la possibilité de combiner, dans la pratique, ces différents dispositifs, avec pour effet une démultiplication de leur impact pour les personnes.* [111]

111. Dans l'affaire *Bridges*, la Haute Cour britannique a considéré que l'utilisation de technologies de reconnaissance faciale par la police

> *va beaucoup plus loin que la simple prise d'une photo. Les informations numériques qui composent l'image sont analysées et les données biométriques du visage sont extraites. Ces informations font ensuite l'objet d'un traitement supplémentaire lorsqu'elles sont comparées aux informations de la liste de personnes recherchées. Le fait que cela se produise lorsque le réclamant se trouve dans un espace accessible au public ne constitue pas une réponse suffisante.* [112]

---

[111] CNIL, Reconnaissance faciale : pour un débat à la hauteur des enjeux, 15 novembre 2019, p.4., https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

[112] *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341, paragraphe 54, traduit de l'anglais : *'goes much further than the simple taking of a photograph. The digital information that comprises the image is*

Par analogie avec la collecte de photos provenant de sources accessibles au public opérée par Clearview, le fait que ces photos soient publiques ne constitue guère une réponse suffisante. Qui plus est, les personnes dont les photos sont collectées par Clearview ne sont souvent pas conscientes que leur visage est disponible et accessible au public sur internet (en particulier lorsque ces photos ont été mises en ligne par des tiers).

112. Or, comme l'a noté la CNIL, l'échelle de ce phénomène est loin d'être anodine :

> *À la différence d'autres données faisant l'objet de traitements biométriques,* ***les données de reconnaissance faciale sont, potentiellement, disponibles partout****. Les visages des personnes sont en effet collectés et enregistrés dans une multitude de bases de données largement disponibles, qui gardent ainsi des traces de passage des individus, dans le temps et dans l'espace, et qui constituent une source potentielle de comparaison pour tout système de reconnaissance faciale. Plus généralement, toute photographie peut potentiellement devenir une donnée biométrique au prix d'un traitement technique plus ou moins aisé.*
>
> *Cette dissémination des données utilisées par les dispositifs de reconnaissance intervient en outre dans un contexte d'exposition de soi permanente sur les réseaux sociaux et, plus généralement, de porosité entre les usages domestiques, privés et publics de ces données. On mesure ainsi le nombre de données techniquement accessibles et potentiellement mobilisables dans le cadre d'une identification par reconnaissance faciale. C'est une spécificité majeure de la reconnaissance faciale.*[113]

113. Telle que déployée dans les espaces publics à des fins de maintien de l'ordre, la reconnaissance faciale n'interfère pas seulement avec les droits au respect de la vie privée et à la protection des données, elle peut aussi sérieusement affecter l'exercice de droits et libertés fondamentaux tels que la liberté de conscience et d'opinion, la liberté de religion, la liberté d'expression et la liberté de réunion et d'association. Le CEPD a souligné que l'utilisation de technologies de reconnaissance faciale « est fondamentalement une question d'éthique pour une société démocratique », car elle peut « manifestement entraver la liberté d'expression et d'association des personnes ».[114]

114. Dans sa contribution sur l'article 21 du Pacte international relatif aux droits civils et politiques adressée au Comité des droits de l'homme des Nations

---

analysed and the biometric facial data is extracted. That information is then further processed when it is compared to the watchlist information. The fact that this happens when the Claimant is in a public space is not a sufficient response.[112]

[113] CNIL, Reconnaissance faciale : pour un débat à la hauteur des enjeux, 15 novembre 2019, p.7. https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf

[114] CEPD, 'Facial Recognition: A solution in search of a problem?' (28 octobre 2019), https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en. , traduit de l'anglais (*'is fundamentally an ethical question for a democratic society' ; 'obviously chill individual freedom of expression and association')*

unies, PI a souligné combien les nouvelles technologies de surveillance peuvent affecter l'exercice du droit à la liberté de réunion pacifique, de par leur « effet dissuasif sur les individus ».[115] L'Observation générale no 37 (2020) a confirmé cette inquiétude : « Si les technologies de surveillance peuvent être utilisées pour déceler des menaces de violence et donc pour protéger le public, elles peuvent aussi porter atteinte au droit à la vie privée et à d'autres droits des participants et des passants et avoir un effet dissuasif. » Cet effet dissuasif rend la mesure des effets négatifs sur les droits fondamentaux très difficile pour les autorités souhaitant justifier l'utilisation de ces technologies, car c'est un effet invisible.[116] À cet égard, le Haut Commissariat des Nations Unies aux droits de l'homme a recommandé que les États s'abstiennent « en tout temps d'utiliser la reconnaissance faciale pour identifier les personnes qui participent pacifiquement à un rassemblement ».[117]

115. En plus de la reconnaissance faciale, l'outil de Clearview permet d'effectuer une surveillance des réseaux sociaux. La surveillance des réseaux sociaux présente elle aussi des risques importants pour les droits fondamentaux des individus. Les régulateurs et les organes de l'ONU ont souligné la nécessité de respecter des garanties strictes dans le cadre de l'utilisation de ce type de technologie. Dans sa jurisprudence, la CEDH a souligné que « [l]a législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans » l'article 8 de la Convention.[118] Ces garanties doivent régir toutes les opérations de traitement effectuées sur des données à caractère personnel par les autorités publiques, y compris leur collecte, leur conservation ou leur stockage, leur analyse, leur diffusion ou leur divulgation, ou toute autre forme de traitement. Comme l'a souligné la Cour dans l'affaire *Marper* :

> *La nécessité de disposer de telles garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières. Le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées [...]. Le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs [...]. Les considérations*

[115] Privacy International, 'Submission on Article 21 of the International Covenant on Civil and Political Rights' (février 2019), p. 10. Traduit de l'anglais 'chilling effect on individuals', https://privacyinternational.org/sites/default/files/2019-03/Submission%20on%20Article%2021%20of%20ICCPR_0.pdf.
[116] Privacy International, 'Protecting Civic Spaces' (1er mai 2019), https://privacyinternational.org/long-read/2852/protecting-civic-spaces.
[117] HCDH (n 86), paragraphe 53(h).
[118] *S. et Marper c. Royaume-Uni* [GC], App nos 30562/04 et 30566/0 (CEDH, 12 avril 2008), paragraphe 103.

qui précèdent valent tout spécialement lorsqu'est en jeu la protection de catégories particulières de données plus sensibles.[119]

116. De façon générale, la surveillance de masse peut porter atteinte aux droits des personnes à s'exprimer anonymement, à formuler et à partager leurs opinions, à polémiquer, à assister à des rassemblements publics et à obtenir réparation suite à des décisions faisant grief de l'administration. À terme, cela peut conduire les individus à pratiquer l'autocensure en évitant de visiter certains profils de réseaux sociaux, de « liker », de partager ou de « re-tweeter » des messages controversés, de rejoindre certains groupes de discussion ou même d'utiliser certains mots. Une telle situation a le potentiel de profondément altérer la manière dont les individus recherchent de nouvelles informations, élaborent et discutent des idées, et s'organisent autour d'elles.[120]

117. En outre, la collecte et le traitement routiniers d'informations accessibles au public à des fins de renseignement peuvent conduire au type d'abus que nous observons régulièrement dans d'autres formes de surveillance couverte ou d'autres opérations de police. Il peut notamment s'agir du ciblage systématique de certains groupes ethniques et religieux par les forces de l'ordre. En effet, la surveillance en ligne ne permet guère de garantir l'absence de préjugés raciaux ou religieux à défaut de notification, de transparence et de contrôle. Et comme le fonctionnement des services de police est souvent opaque quant à l'utilisation de techniques de surveillance des réseaux sociaux et des sources d'information accessibles au public, il peut être extrêmement difficile pour les particuliers de contester toute utilisation potentiellement illégale de ces données.[121]

118. En effet, toute opération de traitement effectuée par les autorités à partir de DACP d'individus publiées sur les réseaux sociaux à des fins allant au-delà de ce à quoi ces personnes peuvent s'attendre devrait être considérée comme une ingérence grave dans leur droit au respect de la vie privée, en particulier lorsque ce traitement implique l'utilisation d'une technologie de reconnaissance faciale pour recouper des sources d'information. Soutenir le contraire reviendrait à refuser la protection de la vie privée des individus dans l'environnement numérique telle qu'elle leur est garantie par la CEDH, un domaine « où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière ».[122]

B. Violation du premier principe de protection des données : Licéité

---

[119] Id.
[120] Privacy International, 'Protecting Civic Spaces' (n 116).
[121] Privacy International, 'Is your Local Authority looking at your Facebook likes?' (mai 2020), p. 7. https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020.pdf.
[122] *Klass c. Allemagne*, App no 5029/71 (CEDH, 6 septembre 1978), paragraphe 56.

119. En vertu de l'article 87 de la loi Informatique et Libertés, les traitements de données à caractère personnel mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, par toute autorité compétente ne sont licites que si et dans la mesure où ils sont nécessaires à l'exécution d'une mission effectuée pour l'une de ces finalités, et où sont respectées les dispositions des articles 89 et 90.

120. Le I de l'article 89 de la LIL prévoit que si le traitement est mis en œuvre pour le compte de l'État pour au moins l'une des finalités précitées, il est prévu par une disposition législative ou réglementaire. Au titre du II de ce même article, si le traitement porte sur des données dites sensibles, il doit être autorisé par un décret en Conseil d'Etat pris après avis motivé et publié de la CNIL.

121. De plus, l'article 88 dispose que dans le cas d'un traitement de catégories particulières de données, celui-ci est autorisé

> *uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée et soit s'il est autorisé par une disposition législative ou réglementaire, soit s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée.*

122. Enfin, au titre de l'article 90 de ce même texte, si le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, notamment parce qu'il porte sur des données dites sensibles, le responsable de traitement est tenu d'effectuer une analyse d'impact relative à la protection des DACP qu'il adresse à la CNIL avec demande d'avis lorsque le traitement est mis en œuvre pour l'Etat.

123. Dans sa délibération SAN-2021-003 du 12 janvier 2021 concernant le ministère de l'intérieur, la formation restreinte de la CNIL estimait s'agissant de l'utilisation de drones équipés de caméras de surveillance à des fins policières que

> *les traitements mis en œuvre en l'espèce sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Ce risque élevé naît, d'une part, des caractéristiques des drones, qui sont des objets volants embarquant une caméra capable de filmer dans des résolutions importantes, en tout lieu et à tout moment. Ils sont donc capables de filmer toute personne circulant dans l'espace public, de la suivre et de traiter des données personnelles intangibles telles que les traits de son visage. Le risque naît, d'autre part, de l'utilisation faite des drones par le ministère de l'intérieur, notamment lors de manifestations, occasions au cours desquelles les opinions politiques, les convictions religieuses ou philosophiques des personnes, ou leur appartenance syndicale, sont susceptibles d'être révélées. Enfin, le risque est aggravé par le fait que les*

traitements sont potentiellement mis en œuvre à l'insu des personnes, celles-ci n'étant souvent pas conscientes de la présence de drones, de l'activation de la caméra et de la captation de leur image. Ce risque est à cet égard aggravé, en l'espèce, par l'absence d'information des personnes à l'occasion des vols réalisés. [123]

124. Par analogie, l'utilisation de l'outil de reconnaissance faciale de Clearview comporte des risques similaires. En effet, laisser des images de soi sur des parties d'internet ouvertes au public peut se rapprocher du simple fait de circuler dans l'espace public. De même, les individus ne sont pas toujours conscients de la présence de leurs images en ligne comme de l'utilisation qui pourrait en être faite par Clearview. Ils n'en sont, par ailleurs, pas davantage informés. Cependant, une différence cruciale fait de la technologie de Clearview un outil de surveillance de masse portant atteinte à la vie privée à une échelle beaucoup plus importante que les drones : non seulement les images traitées par l'outil sont très souvent liées à d'autres informations telles que le nom, la profession, le réseau relationnel ou des catégories particulières de DACP, mais surtout, chacun est susceptible d'être inclus dans la base de données de Clearview. Aussi, en pratique, la société inscrit tout le monde sans distinction sur une liste de personnes recherchées.

125. Dès lors, en raison de la nature de l'outil de Clearview telle que décrite tout au long de cette réclamation et caractérisée par une collecte généralisée et indifférenciée de données biométriques conservées pour une durée indéterminée, PI estime que toutes les conditions et garanties nécessaires pour autoriser son utilisation ne sauraient être satisfaites.

126. La partie suivante de la présente réclamation expose les raisons pour lesquelles dans l'éventualité d'une utilisation de l'outil de Clearview par les autorités répressives, celle-ci ne saurait répondre aux exigences strictes des articles 87 et suivants de la LIL. En effet, un tel usage :

(a) N'est nullement prévu par les textes (législatifs ou réglementaires) – art. 89 paragraphe 1 ; et
(b) Ne saurait satisfaire l'exigence de nécessité absolue – art.88

Aucun texte n'autorise l'utilisation de l'outil Clearview en France

127. Dans sa décision du 18 mai 2020 sur la surveillance par drones, le Conseil d'État a jugé que

[c]ompte tenu des risques d'un usage contraire aux règles de protection des données personnelles qu'elle comporte, la mise en œuvre, pour le compte de l'Etat, de ce traitement de données à caractère personnel sans l'intervention préalable d'un texte réglementaire en autorisant la création et en fixant les modalités d'utilisation devant obligatoirement être respectées

[123] CNIL, Délibération SAN-2021-003 du 12 janvier 2021, paragraphe 44.

ainsi que les garanties dont il doit être entouré caractérise une atteinte grave et manifestement illégale au droit au respect de la vie privée.[124]

128. Dans sa très récente décision du 20 mai 2021 portant sur la « Loi Sécurité Globale », le Conseil constitutionnel a aussi jugé que les dispositions autorisant l'utilisation de drones par la police pour capter des images dans les lieux publics sont contraires à la Constitution.[125] Le Conseil constitutionnel a notamment considéré que les dispositions permettant « la captation et la transmission d'images concernant un nombre très important de personnes, y compris en suivant leur déplacement, dans de nombreux lieux et, le cas échéant, sans qu'elles en soient informées » portent atteinte au droit au respect de la vie privée.[126]

129. Il résulte qu'aucun texte (législatif comme réglementaire) ne vient autoriser et encadrer les traitements de données à caractère personnel qui pourraient résulter de l'utilisation par le ministère de l'intérieur d'un outil tel que celui développé par Clearview – et que tout texte visant à autoriser l'utilisation d'une technologie captant un si grand nombre d'images et permettant la surveillance de personnes dans un vaste périmètre sans qu'elles en soient informées, ne saurait être constitutionnel.

130. Aussi, si la CNIL, lors de ses vérifications suite à la présente réclamation, venait à constater l'utilisation de l'outil de Clearview par les services de police et/ou de gendarmerie, l'autorité devrait nécessairement conclure a minima à une violation de l'article 89 de la LIL.

L'exigence de nécessité absolue

131. La nécessité exige de la police qu'elle prouve l'existence d'une menace concrète, spécifique et immédiate pour la sécurité nationale ou la sûreté publique, qui justifierait la nécessité de déployer le type de technologie développé par Clearview. La CEDH a appliqué un test de stricte nécessité aux interférences avec le droit au respect de la vie privée dans le contexte de la surveillance secrète. Dans l'affaire *Szabó et Vissy c. Hongrie*, la CEDH a indiqué qu'étant donné « le potentiel des technologies de surveillance de pointe à porter atteinte à la vie privée des citoyens », « il est nécessaire d'appliquer un critère de stricte nécessité ». Pour la Cour :

[a] measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding [of] democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The

[124] Conseil d'État, Ordonnance du 18 mai 2020, n[os] 440442 et 440445, paragraphe 18.
[125] Conseil constitutionnel, Décision n° 2021-817 DC du 20 mai 2021, paragraphe 141.
[126] Id., paragraphes 135-136.

Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity – an approach it considers convenient to endorse (texte disponible en anglais uniquement).[127]

132. Pour la CNIL :

> *[l]a reconnaissance faciale ne peut légalement être utilisée, même à titre expérimental, si elle ne repose pas sur un impératif particulier d'assurer un haut niveau de fiabilité de l'authentification ou de l'identification des personnes concernées et sans démonstration de l'inadéquation d'autres moyens de sécurisation moins intrusifs. La proportionnalité des moyens déployés au regard d'objectifs jugés légitimes constitue également une exigence indépassable. À cet égard, la reconnaissance faciale à la volée, qui repose sur une captation indifférenciée des visages dans un espace déterminé, appelle une vigilance toute particulière. Compte tenu de son ampleur et du degré de surveillance qu'il induit, ce type d'usage appelle une analyse approfondie, dans chaque contexte d'utilisation et objectif par objectif, afin d'apprécier l'adéquation ou non de tels dispositifs d'identification.*[128]

133. PI soutient que l'outil de Clearview ne répondra jamais au critère de stricte nécessité, dans la mesure où son usage n'est autre qu'un coup d'épée dans l'eau. En effet, la police ne pourra jamais être certaine que son utilisation est susceptible de produire une correspondance positive, contrairement à l'emploi de listes de personnes recherchées « traditionnelles », contenant exclusivement des suspects identifiés en tant que tels.

134. Dans le cadre de son examen des mesures de conservation des données, la CJUE a estimé que pour être limitées au strict nécessaire, ces mesures doivent faire l'objet de restrictions qui s'avèrent « de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné ».[129] Or dans le cas de Clearview, le public concerné est en fait l'ensemble de la population : chacun se retrouve inscrit sur une liste de personnes recherchées. Bien que la conservation des données soit effectuée par une société privée plutôt que par les services de police, le même test devrait trouver à s'appliquer : les préjudices identifiés par les tribunaux et les autorités dans la conservation généralisée et indifférenciée restent les mêmes lorsque les autorités répressives disposent d'un accès général à la base de données de Clearview. PI exhorte la CNIL à empêcher les autorités publiques de se soustraire à leurs obligations en matière de droits humains et de protection des données en leur interdisant de recourir à un outil privé dans le cadre de leurs opérations de surveillance sans soumettre au préalable cet outil aux mêmes obligations.

---

[127] App no 37138/14 (CEDH, 13 Octobre 2015), paragraphe 73 (traduction française indisponible).
[128] CNIL, Reconnaissance faciale : pour un débat à la hauteur des enjeux, 15 novembre 2019, p.9.
[129] Affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson*, Recueil 2016, p. I-970, point 110.

135. En outre, la collecte, le stockage et le traitement indifférenciés de photos par Clearview peuvent s'apparenter à une conservation généralisée illégale de données[130]. Les risque d'abus et d'accès illicites dans la manipulation de ces ensembles de données sont considérables, c'est pourquoi la CJUE a estimé qu' « un accès général à toutes les données conservées, en l'absence de tout lien, même indirect, avec le but poursuivi, ne peut être considéré comme étant limité au strict nécessaire »[131].

136. Évaluer la nécessité requiert de prendre en compte le principe de proportionnalité. Comme l'indique le « Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel » du CEPD, la nécessité est en fait soumise à la proportionnalité, de sorte que seule une mesure s'avérant strictement nécessaire doit être soumise à un examen de la proportionnalité.[132] Dans l'*affaire S. et Marper contre Royaume Uni*,[133] la CEDH a analysé une mesure impliquant la conservation généralisée et indifférenciée de données biométriques. Il s'agissait en l'espèce du traitement d'empreintes digitales, d'échantillons ADN et cellulaires, effectué dans le but de détecter des infractions pénales et d'en poursuivre les auteurs. La Cour a observé que :

> *la protection offerte par l'article 8 de la Convention serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part. Pour la Cour, le fort consensus qui existe à cet égard au sein des Etats contractants revêt une importance considérable et réduit la marge d'appréciation dont l'Etat défendeur dispose pour déterminer jusqu'où peut aller l'ingérence dans la vie privée permise dans ce domaine. La Cour considère que tout Etat qui revendique un rôle de pionnier dans l'évolution de nouvelles technologies porte la responsabilité particulière de trouver le juste équilibre en la matière.*[134]

137. Les préoccupations exposées à la section VI.A ci-dessus démontrent l'ingérence grave dans la vie privée, la protection des données et dans d'autres droits fondamentaux des personnes que constitue l'outil de Clearview. Cette ingérence pèse lourdement dans la balance contre tout avantage potentiel de cette technologie. En outre, dans le contexte de la reconnaissance faciale « à la volée », il sera très difficile de trouver un équilibre entre les avantages de cette technologie de surveillance et les atteintes aux droits humains, compte tenu des difficultés à intégrer de manière adéquate l'étendue de celles-ci en raison des effets dissuasifs que fait peser l'emploi de ces technologies sur

---

130 Affaire C-623/17 *Privacy International contre SSFCA et Ors* [2020] ECLI:EU:C:2020:790.
131 Id., paragraphe 78.
132 CEPD, « Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel » (11 avril 2017), p. 5, https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_fr.pdf.
133 App nos 30562/04 et 30566/04 (CEDH, 12 avril 2008).
134 Id., paragraphe 111.

l'exercice des droits fondamentaux. Par exemple, les autorités ne seront probablement pas en mesure d'évaluer le nombre exact de personnes ayant choisi de ne pas assister à un événement public, sacrifiant ainsi leur liberté d'expression et de réunion en raison de préoccupations légitimes liées à l'utilisation abusive de leurs données biométriques par les services de police. Compte tenu de la masse et de la nature généralisée et indifférenciée des données collectées et traitées par Clearview, ainsi que des graves problèmes de droits humains soulevés par le recours à cet outil pour faciliter le déploiement de technologies de reconnaissance faciale, PI soutient que l'utilisation éventuelle de Clearview par les services de police et/ou de gendarmerie ne saurait en aucun cas être proportionnée.

VII. Demandes

138. Pour les raisons susmentionnées, Privacy International demande par la présente à la CNIL d'enquêter pleinement sur cette plainte, conformément aux pouvoirs qui lui sont conférés aux articles 19 à 23 de la loi Informatique et Libertés, afin de déterminer notamment :

    (a) Si la collecte initiale d'images et le traitement de données biométriques par Clearview respecte :
        i. Les principes de transparence et de loyauté, en particulier en ce qui concerne les attentes raisonnables des personnes concernées en matière de respect de la vie privée ;
        ii. L'exigence d'une base légale au titre des articles 6 et 9 du RGPD, en déterminant en particulier si le recours aux bases de l' « intérêt légitime » et du « manifestement rendues publiques » est justifié ;
        iii. Le principe de finalité ;
    (b) Si les services de police et/ou de gendarmerie français utilisent ou sont en passe d'utiliser l'outil de Clearview, auquel cas si ce traitement répond aux exigences de licéité, au regard notamment des risques d'atteinte aux droits et libertés fondamentaux des personnes concernées.

139. PI demande à la CNIL de faire usage de son pouvoir d'injonction en exigeant que Clearview cesse toute opération de collecte et de traitement des données personnelles des personnes concernées dans l'UE, en application de l'article 58, paragraphe 2, point f) du RGPD.

140. Comme indiqué dans la présente réclamation, les activités de collecte et de traitement de données de Clearview ne connaissent pas de frontières, s'étendant potentiellement aux individus de tous les pays du monde. Par conséquent, conformément aux dispositions de coopération et d'assistance mutuelle prévues au chapitre VIII du RGPD, nous invitons la CNIL à se mettre en relation avec d'autres autorités de contrôle de l'UE, afin de mener une enquête conjointe en application de l'article 62 du RGPD. En coopération avec d'autres organisations de la société civile, Privacy International portera ces préoccupations à l'attention des autres autorités de protection des données

ainsi que du Contrôleur européen de la protection des données et du Comité européen de la protection des données.

Privacy International

27 mai 2021