Mise en demeure de Clearview AI par la CNIL: les jalons d'un combat pour le droit à l'anonymat

Caroline Lequesne Roth

Mise en demeure de Clearview AI par la CNIL : les jalons d'un combat pour le droit à l'anonymat

A paraître au Dalloz IP-IT – Avril 2022

Référence : CNIL 26 nov. 2021, décis. MED-2021-134, JO 16 déc.

Mots-clés : données à caractère personnelles – données biométriques - CNIL - mise en demeure – reconnaissance faciale.

Solution : Les investigations menées par la CNIL à l'encontre de la société Clearview AI ont conclu que le traitement de données réalisé par cette dernière méconnaissait le RGPD à deux égards : un traitement illicite de données personnelles (manquement à l'article 6 du RGPD) car leur collecte et l'utilisation des données biométriques s'effectuent sans base légale ; l'absence de prise en compte satisfaisante et effective des droits des personnes, notamment des demandes d'accès à leurs données (articles 12, 15 et 17 du RGPD). En conséquence, la CNIL a mis la société en demeure de : cesser la collecte et l'usage des données de personnes se trouvant sur le territoire français en l'absence de base légale ; faciliter l'exercice des droits des personnes concernées et de faire droit aux demandes d'effacement formulées.

Ce qu'il faut retenir : La mise en demeure de la CNIL réaffirme les frontières démocratiques de la société numérique : la publication en ligne des clichés de nos visages ne vaut pas pour autorisation générale de réutilisation et ne peut fonder, seule, la constitution d'une base de données biométriques à des fins de surveillance publique ou privée.

Observations : Lors de sa mise en demeure prononcée à l'encontre de la Société Clearview AI, le 26 novembre dernier, la CNIL enjoignait cette dernière de mettre en conformité ses activités de reconnaissance faciale avec le droit de la protection des données personnelles. Cette affaire constitue l'une des nombreuses ramifications d'un contentieux réticulaire, qui engage une entreprise technologique parmi les plus sulfureuses de la décennie. La start-up new-yorkaise, fondée en 2016, repose sur un concept tout aussi controversé qu'efficace : se servir des publications des internautes pour constituer, selon ses propres termes, la « plus grande base de données biométriques au monde ». Celle-ci comprendrait à ce jour plus de dix milliards d'images faciales, « webscrapées » sur les sites Internet, notamment sur les réseaux sociaux. Cette base de données alimente un logiciel de reconnaissance faciale qui permet à ses clients d'identifier tout individu sur la base d'une simple photographie. Les activités et services de Clearview AI furent révélés au grand public en 2020, dans une enquête du New York Times (K. HILL, "The Secretive Company That Might End Privacy as We Know It", *The New York Times*, Jan. 18, 2020). L'article rapportait que plus de six cents autorités de par le monde recouraient à ses services ; étaient recensées, parmi elles, des forces de police américaines, canadiennes, ou Interpol

(Plus tard, les polices anglaise, australienne, belge, brésilienne, danoise, espagnole, finlandaise, française, hollandaise, irlandaise, indienne, italienne, lettonne, lithuanienne, maltaise, norvégienne, portugaise, serbe, slovène, suédoise et suisse "Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA", *BuzzFeed*, February 27, 2020. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement#4ldqpgc). Ces révélations faisaient alors écho à la ligne de l'entreprise et le segment sur lequel elle entendait se placer : participer au maintien de l'ordre en facilitant l'appréhension des criminels (comme la société le revendique sur son site « *Clearview AI's revolutionary investigative platform enables quicker identifications and apprehensions to help solve and prevent crimes, helping to make our communities safer.*" https://www.clearview.ai/law-enforcement). Toutefois, des révélations ultérieures mirent à mal sa probité, établissant que la société comptait également, parmi ses clients, de nombreuses entreprises privées (chaînes de magasins, société de sport et de divertissement) et des particuliers fortunés. Les récents brevets déposés par l'entreprise confortent en outre cette dynamique, ces derniers visant une application à destination du grand public. L'activité de l'entreprise raisonne aussi comme le slogan d'une époque : la promesse de la « fin de l'anonymat » au service, indifférencié, des systèmes de surveillance étatique et capitalistique. En dépit des réprobations publiques dont elle fit l'objet, Clearview AI est une société prospère, aux résultats florissants : outre son nombre de clients, la taille de sa base de données a triplé en deux ans. En réponse à cette expansion, une riposte contentieuse s'est engagée en 2021, à l'échelon global. De nombreuses autorités de protection des données ont été saisies : les autorités anglaise (*The United Kingdom Information Commissioner's Office, ICO*) et australienne (*The Office of the Australian Information Commissioner,OAIC*) à l'issue d'une enquête conjointe, ainsi que l'autorité canadienne ont déjà enjoint la société de cesser ses activités sur leur territoire et des enquêtes sont pendantes devant les autorités autrichienne (*Datenschutzbehörde*), grecque (*Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*) et italienne (*Garante per la protezione dei dati personali*). Divers recours contentieux ont de surcroît été introduits devant les juridictions américaines. En France, l'autorité de protection des données a été saisie de trois réclamations, émanant d'organisations spécialisées dans la protection des données personnelles (parmi lesquelles Privacy International, qui a coordonné le dépôt des différentes réclamations au sein des autorités de protection européennes), dont les demandes d'accès et de suppression de données personnelles auprès de la société furent infructueuses. La décision de la CNIL intervient ainsi dans un concert régulatoire et judiciaire qui au-delà des frontières du cas, doit apporter des réponses sociétales majeures aux questions soulevées par l'ère digitale globale : peut-on à la fois participer à celle-ci en revendiquant le droit de ne pas « être reconnu » ? Avec qui consentons-nous de partager nos vies et pour quelle(s) finalité(s) lorsque nous publions en ligne ? La CNIL apporte des réponses sans ambages : affirmant sa compétence (**I**) elle assure la protection des citoyens français en identifiant dans l'activité de Clearview AI plusieurs manquements au Règlement général sur la Protection des Données (RGPD), posant les jalons d'un droit à l'anonymat (**II**).

I. Le bouclier de la CNIL : de la compétence de l'autorité de protection des données

Une des particularités – et l'un des enjeux - de la société numérique tient à la déterritorialisation apparente de ses activités : un traitement de données peut être techniquement réalisé « hors sol » européen, c'est à dire par une société n'ayant pas de siège social établi en son sein ; tel est le cas de Clearview AI. Pour asseoir sa compétence en l'espèce, la CNIL devait ainsi établir que cette déterritorialisation n'est qu'un trompe-l'œil : le traitement de Clearview AI concerne les données à caractère personnel des européens, justifiant l'applicabilité du RGPD (**A**). En outre, le traitement dépassant les frontières françaises, la CNIL devait encore se positionner dans le concert des régulateurs (**B**).

A. Une déterritorialisation en trompe l'œil ou l'applicabilité du RGPD au traitement de Clearview AI

L'applicabilité du RGPD au cas d'espèce était particulièrement contesté par la société Clearview AI, à défaut d'établissement au sein de l'Union Européenne. L'enjeu pour la CNIL était de démontrer que le traitement visait des données à caractère personnel relatives à des personnes concernées sur le territoire de l'Union européenne entraînant un suivi du comportement de celles-ci. Pour fonder la protection européenne, l'autorité adopte une lecture restreinte des dispositions du règlement.

L'application du RGPD supposait en premier lieu que les données traitées constituent des données à caractère personnel, traitées au sein de l'Union européenne. La CNIL identifie trois catégories de données mobilisées dans le cadre de l'activité de la société : « *des photographies publiquement accessibles sur Internet* » ; leurs potentiels métadonnées de géolocalisation et les « *informations dérivées de l'apparence faciale des personnes figurant sur ces photographies* ». Les trois, selon elle, constituent des données à caractère personnel dès lors qu'elles permettent d'identifier une personne. L'autorité conditionne expressément la qualification à la reconnaissance, préfigurant la question de la souveraineté des individus en la matière. Elle prend en outre le soin de préciser que seules certaines d'entre elles constituent des données biométriques. En effet, la définition retenue par l'article 4 du RGPD implique un « traitement » et que les photographies, même du visage, ne sont pas considérées comme relevant, par nature, de cette dernière catégorie (en ce sens le considérant 51 du RGPD). Cette qualification constitue à notre sens un écueil, en ce qu'elle induit potentiellement un régime à double vitesse. Certains chercheurs considèrent en ce sens que le RGPD ne s'oppose pas à la collecte d'image faciales (E.KINDT, "A First Attempt at Regulating Biometric Data in the European Union", *AI NOW, Regulating Biometrics: Global Approaches and Urgent Question*s, 2020, p.66). Si la CNIL ne retient pas cette interprétation, on peut toutefois regrettait qu'elle n'ait pas expressément éclairci ce point. Ajoutons que l'autorité poursuit sa démonstration en établissant que les images

concernent effectivement des personnes situées dans l'Union européenne : les éléments transmis par la société corroborent sur ce point la requête des plaignants.

En second lieu, la mise en œuvre du RGPD supposait que la CNIL assure que le traitement réalisé était lié au suivi du comportement de ces personnes. Cette exigence, prévue à l'article 3 du RGPD, procède de l'extra-territorialité du responsable de traitement, Clearview AI n'étant pas établi au sein de l'Union. Pour y parvenir, l'autorité met en œuvre un raisonnement à double détente : dans un premier temps, elle prend le soin de qualifier le traitement de la société, pour envisager, dans un second, les effets de sa mise à disposition auprès de sa clientèle. La CNIL observe ainsi que le traitement procède d'un croisement de données, qui correspond à une opération de profilage : la société ne se contente pas de croiser photographies et gabarit ; elle opère encore une contextualisation des images, lesquelles, reliées à leur(s) source(s), peuvent également être accompagnées de métadonnées géographiques. Ce profilage est certes partiel - notre empreinte numérique n'étant pas liée à notre seule identité biométrique -, mais il n'est pas moins effectif, et le logiciel de Clearview AI constitue, selon la CNIL, une voie alternative pour y accéder. Aussi, les requêtes entrées par la clientèle permettent de suivre un individu, au départ de sa photographie. Il en résulte que le traitement mis en œuvre relève du champ d'application territorial du RGPD.

B. La CNIL dans le concert des régulateurs

La particularité de cette affaire, à l'image du contentieux stratégique émergeant et sans doute à venir en matière de numérique, tient dans sa dimension transnationale. Comme nous le mentionnons, la CNIL a été saisie d'une plainte déposée parallèlement auprès de quatre autres autorités nationales de protection des données. En outre, le fonctionnement même du système Clearview AI procède de la mise en œuvre d'un traitement transfrontalier. Ces éléments appelaient à s'interroger, dans l'effort de coordination institutionnelle européen, sur la compétence de la CNIL. En l'espèce, et contrairement aux récentes controverses auxquelles la Cour de Justice de l'UE s'efforce d'apporter de la clarté (B. BERTRAND, « La Cour de justice, régulateur de la gouvernance institutionnelle du RGPD », *Actualités Dalloz,* 30 juin 2021), l'interprétation ne laissait pas place aux doutes : conformément à la lecture conjointe des articles 55.1 et 56.1, le système de guichet unique ne s'applique pas à l'espèce, Clearview AI n'étant pas établie sur le territoire d'un État membre de l'Union européenne.
La société est donc potentiellement redevable devant toutes les autorités européennes, tenues aux exigences de coopération et d'assistance mutuelle prévues à l'article 61 du RGPD. L'affaire constitue à cet égard une nouvelle occasion d'en approfondir et d'en renforcer les contours. La CNIL est la première à se prononcer au sein de l'Union, confortant la fermeté des positions anglo-australiennes : à défaut de cessation de ses activités sur les territoires concernés, Clearview AI s'expose à une amende de 17 millions de livres sterling en Grande-Bretagne (soit la troisième

amende la plus importante prononcée par l'ICO). La mise en demeure de la CNIL résulte en outre d'une interprétation stricte du RGPD, qui en identifie trois manquements majeurs.

II. Le droit à l'anonymat

Aussi controversé que soit le système de reconnaissance faciale Clearview AI sur les plans éthique et sociétal, la question de sa non-conformité au RGPD laissait apparaître quelques ambiguïtés. L'affaire invitait aussi la CNIL, en toile de fond, à prendre position sur les contours d'un droit à l'anonymat dans la société du numérique. Elle en établit les jalons sur le fond, en reconnaissant que le traitement réalisé par Clearview AI est dépourvu de base légale (**A**), et sur les moyens de sa mise en œuvre en condamnant l'entrave mise en œuvre par la société dans l'exercice des droits des personnes concernées (B).

A. Illégalité du traitement de reconnaissance faciale par Clearview AI

Le traitement de données examiné par la CNIL se décompose, selon cette dernière, en deux temps : Clearview AI collecte de manière « systématique et généralisée » les images contenant des visages accessibles en ligne, pour, dans un second temps, constituer une base de données biométriques ; celle-ci sert de support aux requêtes d'identification soumises à son logiciel. La CNIL relève que le traitement poursuit des fins « exclusivement » commerciales.
La nature des traitements conduit en premier lieu l'autorité à écarter les fondements juridiques prévus par les dispositions de l'article 6.1b), c), d), e) du RGPD liées à l'exécution d'un contrat, au respect d'une obligation légale, à la sauvegarde des intérêts vitaux de la personne concernée et à l'exécution d'une mission d'intérêt public. La CNIL observe en second lieu que Clearview AI ne recueille nullement le consentement des personnes concernées, excluant l'application de l'article 6.1a).

Si la société ne justifiait elle-même d'aucune base légale, on pouvait s'interroger quant à l'opportunité de l'article 6.1f) du RGPD, qui autorise le traitement de données personnelles « nécessaires aux fins d'intérêts légitimes poursuivis par le responsable du traitement » ; la question se posait avec autant d'acuité que les données mobilisées étaient publiquement accessibles : au titre de son intérêt économique, une entreprise peut-elle légalement exploiter des données rendues publiques ? La CNIL répond par la négative aux termes d'un raisonnement en trois temps. Premièrement, elle rappelle que l'accessibilité des données, leur caractère public, n'influe nullement sur la qualification de données personnelles et les garanties qui en découlent. Deuxièmement, elle affirme dans la continuité de sa jurisprudence relative au démarchage commercial (C. CRICHTON, « Démarchage et collecte de données accessibles en ligne : bonnes pratiques », *Dalloz Actualités*, 13 mai 2020), que la mise en ligne ne constitue pas un blanc-seing à la réutilisation : « il n'existe aucune autorisation générale permettant de réutiliser et de traiter de nouveau des données à

caractère personnel publiquement disponible, en particulier à l'insu des personnes concernées ». Cette formulation, par la négative, invite à une approche casuistique, à laquelle elle procède dans un troisième temps en évaluant les intérêts légitimes poursuivis par l'entreprise. L'accessibilité des données pouvait, comme elle l'indique sur le fondement des lignes du CEDP, constituer « un facteur pertinent pour conclure à l'existence d'intérêts légitimes ». Pour autant, la mise en balance avec les droits et libertés fondamentales des personnes concernées ne laisse aucune place à cette interprétation : l'« intrusivité particulièrement forte » dans la vie privée des personnes concernées, en sus de l'impossibilité, pour ces dernières, de former toute attente raisonnable quant au potentiel usage de Clearview AI, écarte en tout point le fondement de l'intérêt légitime, commercial ou pécuniaire, de la société. La CNIL en conclut donc à l'illégalité du traitement.
Au-delà de l'espèce, cette prise de position apparaît essentielle sur le terrain du contrat social numérique, dont elle participe à (ré)affirmer les frontières : le partage public, parfois quotidien, des clichés de nos visages ne peut légitimer, ni autoriser de manière générale une surveillance publique ou privée ; le consentement au partage ne peut se comprendre comme un renoncement général à une part de nos droits, même s'il sert, potentiellement, des principes impérieux de maintien de l'ordre. La question qui demeure est celle de l'effectivité de l'exercice des droits.

B. L'exercice des droits face à la reconnaissance (faciale)

Dans la dernière partie de sa décision, la CNIL mobilise enfin les outils du RGPD permettant aux personnes concernées de garantir ce droit à l'anonymat. Elle soutient en ce sens que Clearview AI a manqué à l'obligation de respecter le droit d'accès d'une part, le droit à l'effacement de l'autre.
Pour établir un manquement au premier, la CNIL fait état des réponses de la société à la demande d'accès formulée par l'une des plaignantes de l'affaire. Après sept courriers recommandés, quatre mois d'échanges et la transmission, à la demande de la société, de ses papiers d'identité, la plaignante a obtenu des éléments relativement succincts. Ils consistent, pour l'essentiel, en un résultat de la recherche effectuée sur sa personne par le logiciel, et un renvoi à la politique de confidentialité de Clearview AI. La partialité de la réponse, alliée à la difficulté de l'obtenir, constitue autant de manquements aux articles 15 et 12 du RGPD selon la CNIL. Ceux-ci sont en outre corroborés par une politique de confidentialité qu'elle condamne en raison de la limitation au droit d'accès qu'elle prescrit : la société restreint l'exercice de ce droit à douze mois, sans démontrer que les données ne sont pas détenues au-delà.
Enfin la CNIL considère, sur le fondement de l'article 17 du RGPD, que l'effacement sollicité des données à caractère personnel « était de droit », eu égard à l'illégalité du traitement.

S'il la reconnaissance de ces droits est essentielle, elle n'en demeure pas moins une faible digue face à un environnement juridique encore lacunaire dans la protection des droits des individus. Bien que constitutionnellement interdit aux forces de

l'ordre, l'usage de la reconnaissance faciale par les services de renseignement d'États tiers ou à la sous-traitance privée ne l'est pas (Cons. Const. Décision n° 2021-834 DC du 20 janvier 2022). Or, en témoigne l'affaire Clearview AI, cette sous-traitance apparaît tout aussi répandue que nébuleuse. Se pose ainsi la question de l'effectivité des droits : comment garantir leur respect dans la méconnaissance des usages ? La question traverse actuellement le débat états-unien, où la technologie s'est avérée décisive en plusieurs affaires sans que les personnes concernées n'en soient informées. Certains États s'efforcent aussi de renforcer la transparence des pratiques, avec des résultats, pour l'heure, mitigés (des législations imposant l'information des personnes concernées ont été adoptées dans l'Etat de New-York et à Détroit ; une proposition de loi œuvrant dans le même sens est également en discussion dans les Etats de Washington et de l'Utah « The Hidden Role of Facial Recognition Tech in Many Arrests", *Wired*, March 7th 2022. https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests/). Le débat rappelle ainsi, une nouvelle fois, l'impérieuse nécessité de l'adoption d'un cadre idoine, garantissant la démocratie numérique.

Caroline LEQUESNE ROTH