

Condamnations de Clearview AI pour le traitement automatisé des données personnelles

Description

Lancée en 2017, Clearview AI est une start-up américaine spécialisée dans la reconnaissance faciale. Pratiquant l'extraction systématique de photographies provenant du web et des réseaux sociaux, elle détient une base de données totalisant 20 milliards de clichés moissonnés sur internet.

Grâce à son moteur de recherche biométrique, Clearview peut fournir à ses clients toutes les occurrences d'une photographie téléversée sur sa plateforme, c'est-à-dire une reconnaissance faciale basée sur les photographies dont elle dispose. Largement utilisé aux États-Unis, notamment par le FBI et les forces de l'ordre, le logiciel de Clearview est un outil destiné aux forces de l'ordre pour identifier les auteurs d'infractions et lancer des poursuites à leur encontre. L'aspiration de ces milliards de photographies ne fait l'objet d'aucune demande d'autorisation auprès des personnes concernées.

À la fin de l'année 2022, l'activité de Clearview a été condamnée par les autorités de protection des données personnelles en France (la Commission nationale de l'informatique et des libertés)¹, au Royaume-Uni (The Information Commissioner's Office)², en Italie (Garante per la protezione dei dati personali)³ et en Grèce (The Hellenic Data Protection Authority)⁴. Ces affaires ont été portées devant ces autorités soit par des particuliers qui n'ont pas pu faire valoir leurs droits à la protection des données personnelles, soit par des associations de protection des données. En effet, au-delà de l'activité même de Clearview AI, est également dénoncée sa politique consistant à limiter au maximum l'accès aux données collectées pour les personnes qui le réclament. Mais c'est la collecte généralisée des données à travers toute l'Europe qui a permis aux autorités de la France, du Royaume-Uni, de l'Italie et de la Grèce d'infliger des amendes alors même que Clearview AI n'exerce aucune activité dans ces pays ni dans l'Union européenne. Le simple traitement des données des citoyens de l'Union, non conforme au règlement général sur la protection des données (RGPD), suffit à la mise en place de sanctions.

Devant chacune de ces instances, Clearview AI a avancé les mêmes moyens de défense, à savoir que ces données personnelles sont déjà disponibles sur internet. La publication volontaire de photographies en ligne était, du point de vue de l'entreprise, un élément suffisant pour en permettre la collecte et le traitement par intelligence artificielle (IA). Cet argument ne porte cependant que sur la collecte des données, alors que ce qui était reproché à Clearview AI tenait aussi à la finalité de cette collecte et aux traitements subséquents. Ce seul argument ne répond donc pas à l'exigence fondamentale du RGPD, à savoir le consentement explicite des personnes à la collecte, dans un but précis, suivi de traitements proportionnés à la finalité. Ainsi, alors qu'elles ont été rendues par des autorités différentes dans des cadres légaux différents, on

constate une certaine unité de ces décisions quant à la protection des données personnelles lors d'un traitement automatisé issu de l'intelligence artificielle.

Le contenu des décisions à l'encontre de Clearview AI

Quatre points ont ordonné ces décisions. En premier lieu le traitement était illicite **(a)** ; en deuxième lieu, il y avait une impossibilité pour les personnes d'obtenir un accès effectif à leurs données et d'en demander la suppression **(b)** ; en troisième lieu, est considérée l'impossibilité de mettre en place des standards de protections dans le cadre de l'utilisation de données biométriques **(c)** ; enfin, le manque d'information des personnes sur le fait que leurs données étaient collectées constitue le quatrième point **(d)**.

a. Le manque de base légale pour un traitement automatisé des données reposant sur l'intelligence artificielle

En vertu du RGPD, tout traitement automatisé des données doit être licite⁵. Cette condition permet de déterminer quels sont les traitements de données autorisés afin de les encadrer dans le respect de la protection des données personnelles. L'intelligence artificielle repose intrinsèquement sur un traitement automatisé de données massives, mais la spécificité de Clearview AI tient à la nature des données traitées. Ainsi, ce n'est pas la qualification d'« intelligence artificielle » qui déclenche l'application du RGPD mais la nature des données traitées, en l'espèce des données personnelles.

Dans le cas de Clearview AI, les données sont collectées et traitées automatiquement sans le consentement des personnes auxquelles appartiennent les photographies moissonnées sur l'internet. D'emblée, le traitement ne pouvait qu'être considéré illicite sous l'égide du RGPD. Cela établit que le cadre juridique du RGPD concernant l'intelligence artificielle instaure le principe d'un consentement pour le traitement algorithmique des données personnelles. Néanmoins, une exception peut être admise avec la possibilité, pour l'État, d'autoriser un tel traitement sous le principe de proportionnalité et de l'encadrer juridiquement. Dans le cas d'espèce, l'intelligence artificielle est soumise au principe de consentement de collecte des données. De plus, le fait que Clearview AI n'avait aucune activité au sein de l'UE rend cette base licite défaillante puisque aucun État membre n'a accepté ce traitement.

b. Le défaut d'accès aux données personnelles et l'impossibilité subséquente de leur suppression

Le deuxième point consiste en un non-respect des droits des personnes (articles 12, 15 et 17 du RGPD), qui sont notamment centrés autour de l'exercice du droit d'accès aux données personnelles. Ce droit d'accès a été violé en le limitant aux seules données collectées durant les douze mois précédant la demande ; en ayant restreint sans justification légitime l'accès à deux fois par an ; et en ne répondant pas à certaines demandes (à l'exception des demandes d'une même personne considérées « excessives »). Ce défaut d'accès ne permettait pas de déterminer l'étendue des données utilisées par Clearview AI, et *a fortiori* ne permettait pas de demander leurs suppressions.

Dans le cas de Clearview AI, la problématique est que le gigantisme de la base de données nécessaire pour entraîner son logiciel d'intelligence artificielle rend impossible pour les personnes concernées de déterminer avec précision quelles sont les données qui ont été collectées. L'accès difficile aux données personnelles révélé par Clearview AI a démontré cette problématique. Celle-ci s'impose à la fois sous l'angle de la technologie, mais également sous l'angle de la politique de l'entreprise, cette dernière étant d'autant plus critiquable quand les moyens techniques d'opérer cet accès sont présents.

En effet, le cadre imposé par Clearview AI, à savoir une forte restriction à l'accès des données personnelles, empêche le plein exercice de ce droit. Les développeurs en intelligence artificielle doivent être contraints de prévoir un cadre pour accéder aux données conformément au RGPD. Cependant, le futur projet de règlement de l'intelligence artificielle (RIA) ne prévoit pas cet accès aux données personnelles. Il convient alors de se demander si la portée de l'accès aux données dans le cadre du RGPD s'exercera encore sur les systèmes d'intelligence artificielle malgré l'introduction du RIA.

c. L'impossible consentement à la collecte des données personnelles

Le troisième axe de condamnation de Clearview AI est que cette collecte de données personnelles est réalisée à l'insu des personnes concernées. Le consentement est la pierre angulaire du RGPD. Cependant, il convient de s'interroger sur la compatibilité entre l'intelligence artificielle et le consentement à l'utilisation des données, compte tenu de la nécessité absolue pour l'efficacité d'une IA de disposer d'une quantité massive de ces données. La question se pose, par conséquent, de savoir si l'intelligence artificielle doit nécessairement obtenir l'autorisation pour le traitement de toutes les données qu'elle entend traiter.

Cette obligation imposée par le RGPD n'est pas reconduite dans le cadre spécifique de l'intelligence artificielle, lequel requiert seulement la nécessité de s'assurer que les données collectées sont représentatives d'une certaine qualité⁶. Le critère de la qualité se rattache à l'exactitude des données collectées ainsi qu'à une calibration adéquate permettant à l'intelligence artificielle d'émettre une solution représentative de la réalité. Si le futur règlement européen relatif à l'intelligence artificielle (RIA) est présenté comme complémentaire au RGPD, la pratique de l'intelligence artificielle et la nécessité de protéger les données personnelles semblent pourtant divergentes. Alors que le RGPD est fondé sur une approche restrictive de l'utilisation des données personnelles⁷, l'intelligence artificielle, à l'opposé de ce principe, requiert la collecte du plus de données possibles. La connaissance de la collecte des données personnelles par les

personnes concernées semble s'amenuiser avec l'utilisation de l'intelligence artificielle.

d. La nécessité d'adopter des standards de protection pour l'utilisation des données biométriques

Il s'agit ici de la finalité de l'intelligence artificielle, à savoir, dans le cas étudié, la reconnaissance d'une personne physique à travers un jeu de données. L'utilisation de Clearview AI ne répondait ni aux standards de protection selon la loi britannique ni au RGPD. Dans le cadre du RGPD, un tel traitement des données à des fins biométriques doit être autorisé par la loi de l'État membre et être proportionné à la finalité définie au préalable.

Les données sont utilisées par des forces de police outre-Atlantique dans le cadre de procédures pénales. L'essor de l'intelligence artificielle dans ces domaines demande des standards supérieurs correspondant à une utilisation à « haut risque » de cette technologie⁸. Ces standards regroupent notamment des exigences de transparence et de contrôle de l'efficacité de l'intelligence artificielle. Ces obligations sont adressées aux fournisseurs de logiciels d'intelligence artificielle, qui rassemblent tant les développeurs que les entités qui la mettent à disposition.

Le RGPD et le RIA ont en commun cette nécessité d'instaurer des standards forts dans l'utilisation de l'intelligence artificielle à des fins précises. Le fondement juridique est néanmoins sensiblement différent, l'intelligence artificielle étant fondée sur une approche basée sur le risque. L'essentiel des obligations se situent par conséquent en amont de leur utilisation, tandis que le RGPD fonde des obligations pendant le traitement des données lui-même et de sa finalité. Dans cette optique, le RIA et le RGPD sont complémentaires.

Quelles sont les perspectives du régime de l'intelligence artificielle en Europe dans le cadre des données personnelles ?

Les conséquences des décisions de justice résultèrent en l'obligation pour Clearview AI de supprimer toutes les données concernant les résidents du Royaume-Uni, d'Italie, de Grèce et de France, ainsi que de s'acquitter d'amendes pour leurs violations des cadres légaux de protection des données. Néanmoins, il convient de noter que ces sanctions ont été prises au regard du seul RGPD. Par conséquent, il faudrait s'interroger au sujet de la prochaine réglementation de l'intelligence artificielle et du risque de provoquer une incompatibilité de ces textes.

En effet, bien que le RGPD et l'IA ne soient pas considérés comme concurrents, leurs finalités divergent fondamentalement. Le traitement des données minimalisé sous le RGPD s'oppose à la logique inhérente à l'intelligence artificielle de traiter le maximum de données possibles. En effet, les caractéristiques intrinsèques de l'IA, fondée sur une maximisation du traitement des données (qu'elles soient ou non personnelles) entraînent des incompatibilités avec l'essence du RGPD. L'ère du big data induit ainsi un certain paradoxe à vouloir réguler l'IA selon le RGPD. Puisqu'il s'agit d'un traitement des données, c'est le

RGPD qui s'applique actuellement. Cependant, celui-ci serait remplacé par un nouveau règlement, en vertu de la doctrine de la *lex specialis*.

Malgré ces divergences, le cadre européen entend établir une certaine complémentarité entre le RGPD et le RIA⁹. Si le RGPD doit s'appliquer aux systèmes de l'intelligence artificielle, cela risque de limiter considérablement l'effectivité de celle-ci, notamment eu égard à la collecte des données.

Dans ce cadre, l'utilisation de milliards de données par l'intelligence artificielle devrait requérir le consentement de tous, ce qui est très irréaliste. C'est cette confrontation de deux logiques diamétralement opposées qui a mené Clearview AI à avancer pour unique voix de défense la seule présence de ces données sur internet. Car, pour tout développeur d'intelligence artificielle, la maximisation de la collecte tient au fonctionnement normal de celle-ci. Il s'agit d'une nécessité intrinsèque à la viabilité et à l'efficacité de l'intelligence artificielle. Tandis qu'au regard du RGPD, il s'agit d'une violation des droits des personnes que de collecter ces données sans leur autorisation.

Assistera-t-on à un conflit insoluble entre règlements lors de l'avènement de celui sur l'intelligence artificielle ? L'effectivité de l'intelligence artificielle est-elle fondamentalement incompatible avec le RGPD ? N'est-il pas possible d'imposer à l'IA un régime aussi strict que celui du RGPD sans diminuer son efficacité ? Il reste inenvisageable de laisser une intelligence artificielle aspirer les données de millions d'Européens à leur insu, ce qui reviendrait à annuler purement et simplement leurs droits conférés par le RGPD.

Il conviendra alors de déterminer un régime de protection des données personnelles propre à l'intelligence artificielle : soit en l'incluant dans une nouvelle rédaction du RIA ; soit par un régime dérogatoire du RGPD comprenant l'intelligence artificielle, au risque de dénaturer gravement la portée du règlement dans son ensemble. Reste donc à élaborer ce régime des données personnelles propre à l'intelligence artificielle, qui devra nécessairement assurer la protection des personnes tout en préservant l'efficacité de l'intelligence artificielle : un équilibre difficile à trouver.

Sources :

1. Cnil, délibération de la formation restreinte n° SAN-2022-019 du 17 octobre 2022 concernant la société CLEARVIEW AI.
2. ICO, enforcement notice addressed to Clearview AI inc, 18th of May 2022, enforcement powers of the information commissioner.
3. GPDP, ordinanza ingiunzione nei confronti di Clearview AI, 10 febbraio 2022.
4. The Hellenic Data Protection Authority, decision 35/2022, 13 July 2022.
5. Parlement européen et Conseil, règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, du 27 avril 2016, 2016/679, article 6.
6. Parlement européen et Conseil, proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle, du 21 avril 2021, COM (2021) 206 final, article 10.

-
7. Parlement européen et Conseil, règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, du 27 avril 2016, 2016/679, considérant 78.
 8. Parlement européen et Conseil, proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle, du 21 avril 2021, COM (2021) 206 final, considérant 38.
 9. Parlement européen et Conseil, proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle, du 21 avril 2021, COM (2021) 206 final, p. 4.

Categorie

1. Droit

date créée

30 mai 2023

Auteur

theoantunes