Quelques photos sur internet suffisent à créer un gabarit biométrique – Mise en demeure de Clearview AI

Alexandre Barbey, le 11 mars 2022

Dans une décision de mise en demeure rendue à l'encontre de la société américaine Clearview AI, la CNIL a constaté que la commercialisation d'un logiciel de reconnaissance faciale développé sur la base de photographies librement accessibles ne repose pas sur une base juridique et est donc illicite.

La CNIL a publié en décembre 2021 une décision de mise en demeure à l'encontre de la société américaine Clearview AI. Cette dernière commercialise un logiciel de reconnaissance faciale principalement pour les forces de l'ordre américaines. Bon nombre d'autorités de protection des données à travers le monde s'y sont intéressées, y compris notre Préposé fédéral à la protection des données et à la transparence (27e Rapport d'activités 2019/20, p. 23).

En naviguant sur le site web de la société Clearview AI, les slogans et témoignages font rêver. Le logiciel développé permettrait d'élucider de nombreuses affaires criminelles aux États-Unis. Plus de 3 000 services de police américains l'utilisent. Et pourtant, malgré ses traits de gendre idéal, de nombreux problèmes ont été identifiés.

Le processus de création du logiciel de reconnaissance faciale consiste à recueillir et ajouter à une base de données toutes les photographies et images extraites de vidéos librement accessibles sur lesquelles figurent des personnes. Des données biométriques en sont extraites et le logiciel développé permet ensuite d'effectuer une recherche par image, en l'occurrence avec la photographie de la personne que l'on cherche à identifier. Le résultat présente toutes les photographies stockées par Clearview sur lesquelles figure la personne, avec l'URL lié et les métadonnées de l'image, en particulier les données géographiques lorsque celles-ci sont disponibles.

Ce procédé a permis à Clearview d'enregistrer jusqu'à maintenant environ dix milliards d'images. À titre de comparaison, le FBI n'aurait en sa possession « que » 411 millions d'images, soit environ 24 fois moins (New York Times du 18 janvier 2020).

L'application du RGPD

Comme la société Clearview AI n'est pas établie et n'offre pas ses services dans l'UE (art. 3 par. 2 let. a RGPD), mais traite néanmoins des données personnelles relatives à des personnes concernées se trouvant sur le territoire de l'Union, la CNIL examine dans un premier temps si son activité pouvait être qualifiée de suivi comportemental au sens de l'art. 3 par. 2 let. b RGPD.

Ainsi, la CNIL a tout d'abord constaté que Clearview traitait effectivement des données personnelles, à savoir les photographies sur lesquelles apparaissent des personnes et les données biométriques qui en ont été extraites. En outre, une partie de ces personnes se trouvaient sur le territoire de l'UE.

Afin de déterminer s'il existe un suivi comportemental, la CNIL relève qu'en plus des photographies, d'autres informations sont disponibles dans les résultats de recherche, en particulier le site web sur lequel figure l'image et les données de localisation. Cela permet d'obtenir bien plus d'informations à propos de la personne recherchée. Partant, la CNIL considère que Clearview a procédé à un profilage des personnes concernées (art. 4 ch. 1 RGPD) . De plus, considérant les moyens utilisés pour créer le logiciel, l'autorité française considère que ce traitement est « lié au suivi du comportement » des personnes et que, au vu de l'automatisation du traitement, il s'agit d'un suivi sur internet. Partant, le RGPD s'applique au traitement de données effectué par Clearview (art. 3 par. 2 let. b. RGPD).

Au niveau procédural, étant donné que Clearview n'est pas établie dans l'UE, le système du guichet unique de l'art. 56 RGPD n'est pas applicable. Ainsi, chacune des autorités des États membres a une compétence propre s'agissant de leur territoire. Pour cette raison, les effets de la décision de mise en demeure de la CNIL sont limités au territoire français. À titre d'exemple, l'autorité italienne de protection des données a rendu le 10 février 2022 une décision condamnant Clearview à une amende de 20 millions d'euros s'agissant de manquements qui ont eu lieu sur le territoire italien.

Les manquements au RGPD

La CNIL constate une violation du principe de licéité (art. 6 RGPD). Elle ne s'est intéressée qu'à la question de savoir si le traitement était nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement (art. 6 par. 1 let. f RGPD), les autres motifs justificatifs ayant été écartés sans autre justification.

Dans la pesée des intérêts effectuée, la CNIL rappelle que le traitement de données personnelles publiquement accessibles est soumis au RGPD ; il n'existe pas de droit général au trai-

tement de ces données, à plus forte raison lorsque les personnes concernées n'en sont pas informées. Un intérêt au traitement de ces données pourrait être légitime s'il est réalisé par exemple dans un but de recherche. Or l'intérêt de Clearview est purement économique. Celui-ci doit être mis en balance avec les intérêts et droits fondamentaux des personnes concernées. La CNIL soutient que le grand nombre de données récoltées ainsi que la création du gabarit biométrique sur cette base constituent une forte atteinte à la vie privée. Un point clé dans le raisonnement est que les personnes publiant sur internet des photographies sur lesquelles apparaît leur visage ne peuvent raisonnablement pas s'attendre à ce qu'elles soient utilisées pour créer un gabarit biométrique et un logiciel de reconnaissance faciale qui soit commercialisé à la police. La majorité ne se doute pas qu'un tel traitement de leurs données peut être réalisé, d'autant plus qu'il ne s'agit pas d'un logiciel auquel tout un chacun peut accéder. Il n'y a donc pas d'intérêt légitime de Clearview AI au traitement de ces données. Partant, le traitement est illicite.

La CNIL constate également deux autres manquements. Tout d'abord, les droits d'accès des personnes concernées n'étaient pas respectés (art. 15 RGPD). Des tests ont démontré qu'il faut attendre plusieurs mois et un nombre non négligeable de relances pour exercer son droit d'accès. De plus, la société limite ce droit aux données collectées dans les douze mois avant la demande. Enfin, il n'a pas été donné suite aux demandes d'effacement des données quand bien même le traitement est illicite (art. 17 par. 1 let. d RGPD).

Mise en demeure

Au vu de tous ces éléments, la CNIL a ainsi mis en demeure Clearview de cesser son traitement, de supprimer les données enregistrées et de faciliter les droits d'accès et répondre aux demandes d'effacement des données. Un délai de deux mois avait été imparti à la société pour se mettre en conformité. Ce délai est aujourd'hui écoulé. La CNIL n'a depuis plus communiqué sur cette affaire et n'a notamment pas publié la clôture de la procédure (art. 20 II Loi Informatique et Libertés). Nous pouvons donc raisonnablement penser que Clearview ne s'est pas conformée à la décision de mise en demeure.

Analyse

Il est choquant de constater qu'une société privée ait pu extraire les données biométriques d'une très grande partie de la population mondiale sans réel obstacle autre que financier, qu'elle offre ses services aux autorités policières américaines et que ce faisant elle ne respecte pas les droits des personnes concernées. Même si Clearview se vante des exploits que sa technologie a permis d'obtenir dans des enquêtes pénales, un risque d'utilisation frau-

duleuse existe au vu du nombre d'autorités de forces de l'ordre qui ont accès à ce logiciel. De plus, même si les mesures de sécurité nécessaires relatives à l'emploi de ce logiciel sont prises, rien n'empêche des tiers de le créer à nouveau, la matière première du logiciel étant librement disponible, et de l'utiliser avec de mauvaises intentions.

Que peut-on faire ? Le PFPDT recommande dans son rapport d'activité que les utilisateurs ne laissent pas leurs profils publics afin qu'on ne puisse pas y avoir accès sans être inscrit sur la plateforme en question. Cela ne résout cependant le problème que pour les photographies qui seront publiées une fois le profil devenu privé. En effet, Clearview conserve les photographies auxquelles elle a eu accès. Ainsi, même la suppression de photographies par les personnes concernées n'est pas suffisante.

Cette affaire révèle que, désormais, ce n'est plus simplement le fait de ne pas publier de photo compromettante qui pourrait se révéler problématique pour celui qui figure dessus, mais que n'importe quelle photographie publiée sur internet en libre accès peut permettre à autrui de créer un profil de la personnalité. De plus, ce logiciel, a priori très performant, a en réalité un taux d'erreur qui dépend de l'origine ethnique de la personne que l'on recherche, ce qui peut amener à de nombreuses complications, spécifiquement dans le cadre d'une procédure pénale.

En Suisse, les forces de l'ordre semblent ne pas être intéressées par l'utilisation de ce logiciel de reconnaissance faciale (27e Rapport d'activités 2019/20, p. 23). Le traitement de données par Clearview pose également de nombreux problèmes sous l'angle de la (n)LPD et le traitement serait également illicite en droit suisse. Si le logiciel était néanmoins utilisé par les autorités pénales suisses, nous considérons que des problèmes de procédure pénale se poseraient. Nous sommes d'avis que la règle sur l'exploitation des moyens de preuve obtenus illégalement de l'art. 141 al. 2 CPP trouverait application en l'espèce, en faisant spécialement référence aux art. 260 ss CPP qui règlementent la saisie, l'utilisation et la conservation de données biométriques par les autorités pénales (dites signalétiques en matière de droit pénal suisse) et 282 ss CPP, relatifs aux mesures de surveillance secrètes d'observation. Les données signalétiques doivent en pratique être prélevées par la police et en aucun cas par une société privée (CR–CPP ROHMER/VUILLE, art. 260 N 20 et 20a ; JEANNERET/KUHN, *Précis de procédure pénale*, 2e éd., Berne 2018, N 14064). De plus, le CPP s'applique lorsqu'une infraction a été commise, et non pas en amont de toute infraction afin d'identifier tout un chacun. La personne concernée est au courant du traitement de ses données. Enfin, le principe veut que les données soient conservées dans le dossier pénal, et non pas dans une base de données accessible à distance par n'importe qui.

Proposition de citation : Alexandre BARBEY, Quelques photos sur internet suffisent à créer un gabarit biométrique – Mise en demeure de Clearview AI, 11 mars 2022 *in* www.swissprivacy.law/130