La Présidente

MINISTERE DE L'INTERIEUR
MONSIEUR LE MINISTRE
1 PLACE BEAUVAU
75008 - PARIS

Paris, le 30 mars 2020

N/Réf. : [redacted]/DI201106
A rappeler dans toute correspondance

Monsieur le Ministre,

Différents articles de presse internationale ont récemment fait état de l'utilisation, notamment par des services de police, d'une application de reconnaissance faciale dénommée Clearview AI commercialisée par la société Clearview AI, Inc. établie aux Etats-Unis.

Ces articles indiquent que cette société aurait constitué une base de données de trois milliards d'images de personnes et d'éléments d'identification associés. Ces informations seraient collectées sur internet, notamment sur les réseaux sociaux. Pour utiliser cette application, il suffirait de soumettre au système une image dont on dispose au format numérique, en vue de rechercher des correspondances dans la base permettant le cas échéant d'identifier la personne concernée. Les recherches peuvent s'effectuer à partir de photographies de visages mais également de vidéos.

Il ressort également de plusieurs articles que la société Clearview AI Inc. aurait fait l'objet d'une violation de données ayant affecté sa base de données et la liste de ses clients. Le média en ligne Buzzfeed News aurait ainsi eu accès à cette liste et a indiqué dans un article en date du 27 février 2020 (https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement) que les forces de police de 27 pays, dont la France, feraient partie des utilisateurs de l'application.

Par un courrier en date du 22 janvier 2020, des parlementaires européens ont saisi le Comité Européen à la Protection des Données (CEPD) concernant ce dispositif de reconnaissance faciale. Les parlementaires dénoncent notamment le manque de transparence lié au développement d'une telle application, estimant qu'il existe une menace réelle pour les droits fondamentaux des citoyens et la démocratie. Les parlementaires ont également interrogé le CEPD afin de savoir si, à sa connaissance, l'application Clearview AI était utilisée par des services de police de pays européens et si des images de ressortissants européens figuraient dans la base de données. Ils souhaitent enfin savoir si l'usage, par des services régaliens, d'une application de reconnaissance faciale proposée par un opérateur privé, était conforme à la règlementation européenne en matière de protection des données.

Des travaux sont actuellement menés par les autorités de protection des données afin d'apporter, de manière concertée, des éléments de réponse tant aux parlementaires européens qu'aux éventuelles réclamations ou interrogations dont elles auraient été ou seront saisies. A ce titre, l'autorité de protection des données suédoise, Datainspektionen, a décidé d'initier des investigations sur son territoire afin, notamment, de déterminer si les services de police suédois ont eu recours à l'application en question.

Il m'est apparu important, dans ce contexte, de vérifier auprès de vous si des services de police ou de gendarmerie français ont effectivement eu recours à cette application et, le cas échéant, pour quel usage, en vous alertant sur les questions qu'un tel recours serait susceptible de soulever.

En effet, au vu des éléments dont la CNIL dispose, le traitement proposé par la société Clearview AI Inc. n'apparaît pas conforme à la législation sur la protection des données à caractère personnel sur plusieurs points, tant s'agissant des modalités de collecte des données sur internet, que de leur utilisation dans le cadre d'un dispositif biométrique à des fins d'identification.

D'une part, aucun texte ne vient encadrer un tel usage, alors que l'article 32 de la loi Informatique et Libertés exige l'autorisation préalable par un décret en Conseil d'Etat, pris après avis de la CNIL, pour tout traitement mis en œuvre pour le compte de l'Etat agissant dans l'exercice de ses prérogatives de puissance publique et portant sur des données sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes. Il n'est possible de se dispenser d'un tel texte que lorsqu'il s'agit de protéger les « intérêts vitaux d'une personne physique » ou lorsque le traitement porte sur des données « manifestement rendues publiques » par la personne concernée. Aucune de ces deux exceptions n'apparaît aisément mobilisable dans la généralité des cas d'usage de l'application Clearview. En particulier, j'attire votre attention sur le fait que, selon, le Comité européen de la protection des données (CEPD), le simple fait que des données soient publiquement accessibles sur les réseaux sociaux ne permet pas de considérer qu'elles ont été « manifestement rendues publiques » par la personne[1].

D'autre part, sur le fond, le recours à une telle application pose question au regard de l'article 88 de la même loi « informatique et libertés », qui subordonne le traitement de données sensibles telles que les données biométriques, dans le champ de la directive « police justice », à la preuve – qui devrait être apportée - d'une « nécessité absolue » et à des « *garanties appropriées pour les droits et libertés de la personne concernée* ».

Au regard de l'ensemble de ces éléments, les conditions de l'éventuel recours à un tel dispositif par les forces de l'ordre françaises à des fins opérationnelles, notamment d'enquête, n'apparaissent, en l'état, pas réunies.

Les services de la Commission restent à la disposition des vôtres pour tout échange sur les points soulevés dans le présent courrier, en particulier sur l'usage d'une telle application qui aurait pu être fait par votre ministère.

Je vous prie d'agréer, Monsieur le Ministre, l'expression de ma haute considération.

M-L. De

Marie-Laure DENIS

---

[1] Dans son avis sur certaines questions clés de la directive (UE) uis endossée par le Comité Européen à la Protection des Données (CEPD) - indique que « *cet article doit être interprété comme impliquant que la personne concernée a été informée du fait que les données respectives seront rendues publiques pour tout le monde, y compris les autorités* ». Il est précisé qu'en cas de doute, une interprétation restrictive devrait prévaloir. S'agissant de l'inscription à un réseau social, même si une telle information est prévue, cela reste insuffisant dans la mesure où « *la plupart des utilisateurs ne prennent pas activement connaissance de ces règles et ignorent en fait que leurs données sont mises à la disposition des forces de police* ».