DBF Bruxelles
Délégation des Barreaux de France

Droit des technologies de l'information

L'Avis de l'Expert Européen

N°6 MAI 2020

Eric LE QUELLENEC
Avocat au Barreau de Paris
Directeur du département informatique conseil
Membre du Conseil de l'Ordre, co-référent ordinal de l'incubateur du Barreau de Paris

CHIFFRE CLÉ

3 mois

Durée de l'expérimentation de la reconnaissance faciale pour le port du masque station Châtelet, soit jusqu'en août 2020

- **Directive (UE) 2016/680** du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection, et abrogeant la décision-cadre 2008/977/JAI du Conseil
- **Règlement (UE) 2016/679** du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Pour aller plus loin

Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) du Conseil de l'Europe
- Rapport sur l'intelligence artificielle – Intelligence artificielle et protection des données : enjeux et solutions possibles

Commission Nationale de l'Informatique et des Libertés
- Directive « Police-Justice » : de quoi parle-t-on ?
- Comment permettre à l'Homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle

Commission européenne
- Livre blanc sur l'intelligence artificielle

Conseil des Barreaux européens
- Considérations du CCBE sur les aspects juridiques de l'intelligence artificielle

La Quadrature du Net
- La Quadrature Du Net attaque l'application Alicem, contre la généralisation de la reconnaissance faciale
- Reconnaissance faciale : entre exigence de contrôle et respect de la vie privée – Quels outils, quels enjeux, quelles garanties ?

L'utilisation de la reconnaissance faciale

Le 21 février 2020, selon plusieurs sources concordantes, les forces de police et de gendarmerie de plusieurs pays proposaient à la Commission européenne de mutualiser leurs fichiers pour permettre des traitements de reconnaissance faciale dans le cadre d'enquêtes à l'échelle de l'Union européenne. L'utilisation des photographies lors d'enquêtes de police n'a rien d'innovant. C'est l'usage d'algorithmes pour que la machine, sur la base d'un traitement de l'image en gabarit, puisse effectuer cette reconnaissance d'un suspect à la place de l'agent ou de l'officier de police judiciaire qui constitue un des défis majeurs de ce début du 21ème siècle.

Au niveau national, des expérimentations sont déjà en cours et ont même déjà donné lieu à débat devant le tribunal correctionnel de Lyon. Par jugement du 31 octobre 2019, l'auteur d'un vol de camion et de sa marchandise a été condamné sur la base d'images de vidéosurveillance croisées avec les banques d'images des fichiers TAJ et GASPARD. Même si l'enquête a aussi permis de confondre l'auteur présumé des faits sur la base d'autres éléments de preuve, le défenseur du prévenu n'a pas manqué de souligner que le logiciel permettant d'effectuer le rapprochement n'a pas été dévoilé lors de la procédure. Ainsi, sa légalité pose question bien que l'administration de la preuve soit libre en matière pénale.

Tout logiciel de reconnaissance faciale repose sur des algorithmes qui reposent, eux-mêmes, sur des choix dictés par l'homme. C'est à ce titre que le règlement général sur la protection des données personnelles (dit « RGPD ») et la directive (UE) 2016/680 (dite « directive Police-Justice ») auraient dû être mis en application pour que la protection de la personne soit respectée dès la conception de tels logiciels, conformément aux principes de loyauté et de dignité. A défaut, le manque de transparence de ce type d'outils suscite des interrogations pour au moins quatre raisons :
- Quant à la source des données utilisées, notamment en cas de croisement de fichiers à grande échelle ;
- Au titre de la finalité des traitements, telle que l'utilisation envisagée de la reconnaissance faciale dans le cadre du projet français ALICEM aux fins de l'utilisation de services publics en ligne ;
- Du fait de l'existence potentielle de biais raciaux ou ethniques ;
- En raison des limites techniques de ce type d'outils puisque les faux positifs comme négatifs réduisent leurs performances à moins de 40% de résultats corrects.

Un autre risque tient à la vulnérabilité de ces outils face à des attaques informatiques. Par exemple, la société américaine Clearview vient récemment d'en faire l'expérience puisque les données personnelles qu'elle avait collectées ont été utilisées dans plus de 2200 cas, par des services de police, des agences gouvernementales et des entreprises dans 27 pays.

En France, la CNIL s'est récemment opposée aux dispositifs d'expérimentation prévoyant le recours à la reconnaissance faciale à l'entrée de lycées.

En cette période de pandémie, les applications de géolocalisation mobilisent plus urgemment les autorités européennes, sur des problématiques proches du traitement à grande échelle des déplacements des individus et de leur exposition présumée au virus. Après avis du Comité européen de la protection des données personnelles, la Commission avec les Etats membres, vient de publier une boîte à outils sur les règles et bonnes pratiques pour ce type d'applications.

Il serait tout aussi urgent d'adopter, en matière de reconnaissance faciale, une position européenne convergente et respectueuse des droits fondamentaux.