25.10.2021

Recommandations de l'étude des pratiques de reconnaissance faciale en Europe

Recommandations

1. L'Union Européenne devrait interdire le déploiement des technologies d'identification biométrique et comportementale à distance (RBI) dans les espaces publics, qu'elles soient indiscriminées ou "ciblées" (RBI en temps réel), ainsi que l'identification a posteriori (ou RBI médico-légale). Notre analyse montre que ces deux pratiques, même lorsqu'elles sont utilisées pour une "surveillance ciblée", constituent une surveillance de masse.

- En accord avec les recommandations similaires faites par le Comité Européen de la Protection des Données (EDPB) et le Contrôleur européen de la protection des données (CEPD), l'UE devrait interdire le déploiement des technologies d'identification biométrique et comportementale à distance dans les espaces publics.
- Notre recherche soutient la notion que la distinction entre "temps réel" et "ex-post" n'est pas pertinente quand il s'agit de l'impact de ces technologies sur les droits fondamentaux.
- Cela concerne non seulement l'acquisition et le traitement des visages, mais aussi de la démarche, de la voix et d'autres signaux biométriques ou comportementaux.

2. L'UE devrait renforcer la transparence et la responsabilité des technologies de reconnaissance biométrique et comportementale.

- Nos recherches ont révélé que la majorité des systèmes de surveillance restent opaques. Il existe très peu d'informations sur la manière dont les données des citoyens sont traitées lorsqu'ils pénètrent dans des espaces publics surveillés. Il est rare que des alternatives concrètes soient proposées aux personnes qui ne souhaitent pas être surveillées.
- Il faut donc étendre les exigences de transparence et de responsabilité existantes dans la nouvelle loi européenne sur l'intelligence artificielle aux technologies biométriques pour qu'elles incluent une responsabilité, une transparence et un contrôle externes indépendants pour toute mise en œuvre de technologies biométriques qui ne sont pas déjà interdites par la loi.
- En particulier, il semble impératif d'accroître la transparence de ces systèmes en conditionnant leur fonctionnement à la publication de caractéristiques et d'éléments clés nécessaires à un contrôle public efficace de leur fonctionnement, Ces détails devraient être divulgués même lorsque les déploiements sont utilisés à des fins de sécurité nationale ou d'application de la loi, et le public devrait être informé des projets prévus et en cours.

3. L'UE devrait promouvoir le renforcement de mécanismes de responsabilité solides pour les systèmes de surveillance biométrique.

- Le cadre législatif actuel reste flou quant aux institutions qui peuvent examiner ou autoriser les systèmes de surveillance biométrique.
- L'UE devrait s'efforcer de mettre au point une procédure d'autorisation centralisée pour la surveillance biométrique, dans laquelle toutes les autorités compétentes seraient incluses et pourraient opposer leur veto à l'autorisation.
- Bien que la proposition de loi européenne sur l'intelligence artificielle limite l'autorisation préalable d'un tribunal ou d'une autorité administrative indépendante à la surveillance biométrique "en temps

réel", il est nécessaire de souligner que les systèmes d'identification biométrique a posteriori doivent être soumis à une supervision ou à une autorisation tenant compte des normes de la CEDH et de la Charte.

4. L'UE devrait promouvoir les droits individuels au titre du RGPD par la promotion des technologies de type "droits numériques dès la conception".

- Une plus grande attention pourrait être accordée à la protection des droits des individus au titre du RGPD lorsqu'il s'agit de mécanismes de collecte et de traitement des données ainsi que d'une évaluation des droits fondamentaux ex ante et ex post.
- Cela pourrait être mis en œuvre techniquement par des méthodes de minimisation des données ou de conception des droits numériques, soit par des solutions techniques qui ne collectent pas d'informations biométriques, soit par des systèmes qui intègrent des formes automatisées de notification, de transparence immuable et d'enregistrement des responsabilités, et de contrôle des données ou, idéalement, par une combinaison des deux approches.

5. L'UE doit veiller à l'application effective de la limitation de la finalité du RGPD.

- La limitation de la finalité est l'un des principes clés du RGPD. Comme le montre notre rapport, la réutilisation des données biométriques n'est pas toujours suffisamment contrôlée.
- D'un point de vue technique, la surveillance biométrique de masse peut facilement émerger en connectant différents éléments d'une infrastructure technique (capacités d'acquisition vidéo, algorithmes de traitement, jeux de données biométriques) développés dans d'autres contextes.
- Afin de maintenir un contrôle démocratique sur les utilisations de l'infrastructure et d'éviter le risque de dérive, il est donc impératif que le principe de limitation de l'objectif soit systématiquement appliqué et strictement réglementé en ce qui concerne le type de données sur lesquelles les recherches biométriques peuvent être effectuées.

6. L'UE devrait soutenir les voix et les organisations qui se mobilisent pour le respect des droits fondamentaux de l'UE.

- Nos recherches ont montré que de nombreuses institutions de la société civile s'emploient à faire respecter les droits fondamentaux de l'UE dans le domaine des technologies de sécurité biométrique.
- Si, dans certains pays, elles bénéficient d'un réseau dense de financement de la société civile, dans d'autres, elles sont soumises à une surveillance étroite et à des restrictions financières.
- En particulier dans le domaine des litiges, le soutien à la société civile et à l'accès des citoyens européens aux droits pourrait être extrêmement utile et nous conseillons donc à l'UE de soutenir les initiatives existantes en matière de litiges relatifs aux droits numériques et de créer des mécanismes supplémentaires pour soutenir cette approche.

7. L'UE devrait prendre en compte la dimension mondiale de l'industrie des technologies biométriques et d'analyse comportementale.

- Les technologies de reconnaissance faciale utilisées en Europe proviennent de fournisseurs du monde entier. Les technologies d'analyse biométrique ou comportementale sont souvent testées dans un pays avant d'être mises en œuvre dans un autre.
- La politique de l'UE concernant l'industrie des technologies d'analyse biométrique ou comportementale doit donc tenir compte de son impact à l'intérieur et à l'extérieur de l'Europe. À cet

égard, le cadre de contrôle des exportations de l'UE récemment révisé, qui peut inclure les technologies biométriques et comportementales, peut jouer un rôle.