25.10.2021

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

CHAPITRE 1 : Introduction

- L'objectif de ce rapport est d'établir une vue d'ensemble problématisée des pratiques actuelles en Europe d'identification biométrique à distance (RBI), et d'évaluer dans quels cas nous pourrions potentiellement tomber dans des formes de surveillance biométrique de masse.
- Les acteurs privés et publics déploient de plus en plus de solutions de "surveillance intelligente", y compris des technologies d'identification biométrique à distance qui, si elles ne sont pas contrôlées, pourraient devenir une surveillance biométrique de masse.
- La technologie de reconnaissance faciale a été la plus discutée des technologies RBI. Cependant, il semble que l'on comprenne mal les façons dont cette technologie pourrait être appliquée et l'impact potentiel d'un si large éventail d'applications sur les droits fondamentaux des citoyens européens.
- Le développement de systèmes RBI par des régimes autoritaires qui pourraient ensuite être exportés et utilisés en Europe est préoccupant. Non seulement en ce qui concerne les déploiements de ces technologies, mais aussi en raison du manque d'informations adéquates sur les pratiques de protection de la vie privée des entreprises qui fournissent les systèmes.
- Quatre positions principales ont émergé parmi les acteurs politiques en ce qui concerne les déploiements des technologies RBI et leur impact potentiel sur les droits fondamentaux : 1) la promotion active ; 2) le soutien assorti de garanties ; 3) le moratoire et 4) l'interdiction pure et simple.

CHAPITRE 2 : Aperçu technique

- Le marché actuel des systèmes RBI est largement dominé par les produits basés sur l'image, au centre desquels se trouve la technologie de reconnaissance faciale (FRT). D'autres produits tels que les technologies de détection des visages et des personnes sont également utilisés.
- La FRT est généralement déployée pour effectuer deux types de recherches : des recherches coopératives à des fins de vérification et/ou d'authentification, et des recherches non coopératives pour identifier une personne concernée. Dans le premier cas, la personne concernée doit consentir volontairement à la capture de son image, alors que dans le second, ce n'est pas toujours le cas.
- La reconnaissance faciale en direct est actuellement le déploiement le plus controversé du FRT : les flux vidéo en direct sont utilisés pour générer des clichés d'individus et les comparer ensuite à une base de données d'individus connus - la "liste de surveillance".
- D'autres technologies RBI sont en cours de déploiement, bien que leur utilisation soit pour l'instant marginale par rapport à la FRT. Il s'agit notamment des technologies de reconnaissance de la démarche (mouvement), de l'audio et des émotions, entre autres.
- Une meilleure compréhension des composants techniques et des applications possibles des technologies RBI basées sur l'image est nécessaire afin d'évaluer leurs implications politiques potentielles.

- Les technologies RBI sont sujettes à des défis et des limitations techniques qui doivent être pris en compte dans toute analyse plus large de leurs implications éthiques, légales et politiques.

CHAPITRE 3 : Aperçu des déploiements en Europe

- Les déploiements actuels des technologies RBI en Europe sont principalement expérimentaux et localisés. Cependant, la technologie coexiste avec un large éventail de traitements algorithmiques d'images de sécurité effectués à une échelle allant du niveau individuel à ce que l'on pourrait qualifier de surveillance biométrique de masse. La distinction des différentes caractéristiques de ces déploiements est non seulement importante pour éclairer le débat public, mais elle permet également de concentrer la discussion sur les utilisations les plus problématiques des technologies.
- Les applications de sécurité basées sur l'image et le son et utilisées à des fins d'authentification ne présentent actuellement aucun risque pour la surveillance biométrique de masse. Il convient toutefois de noter qu'une modification du cadre juridique pourrait accroître le risque qu'elles soient déployées à des fins de surveillance biométrique de masse, d'autant que de nombreuses bases de données utilisées contiennent des millions de personnes.
- Outre l'authentification, des applications de sécurité basées sur l'image et le son sont déployées pour la surveillance. Les applications de surveillance comprennent le déploiement de RBI dans les espaces publics.
- Les progrès réalisés sur deux fronts font que le développement de la surveillance biométrique de masse est plus qu'une possibilité lointaine. Premièrement, la création et/ou la mise à niveau actuelles des bases de données biométriques utilisées dans les registres civils et criminels. Deuxièmement, le pilotage répété de systèmes de diffusion en direct connectés à des algorithmes de recherche et de reconnaissance d'informations faciales et biométriques à distance.

CHAPITRE 4 : Bases juridiques

- L'utilisation d'outils biométriques à des fins répressives dans les espaces publics soulève la question essentielle de l'admissibilité juridique de la collecte, de la conservation et du traitement des données au regard des droits fondamentaux de l'individu à la vie privée et à la protection des données personnelles. Considérées sous cet angle, les technologies RBI pourraient avoir un impact grave sur l'exercice d'une série de droits fondamentaux.
- Le déploiement de la surveillance biométrique dans les espaces publics doit faire l'objet d'un examen strict afin d'éviter les circonstances qui pourraient conduire à une surveillance de masse. Il s'agit notamment de la surveillance ciblée qui peut entraîner la collecte indiscriminée de données sur toute personne présente dans le lieu surveillé, et pas seulement sur la personne concernée.
- Le cadre juridique normatif permettant d'effectuer une surveillance biométrique dans les espaces publics se trouve dans la législation secondaire de l'UE sur la protection des données

(RGPD et Directive Police Justice). L'utilisation des données biométriques dans ce cadre doit être examinée à la lumière de la protection offerte par les droits fondamentaux.
- La proposition de règlement de la Commission européenne d'avril 2021 relative à la loi sur l'intelligence artificielle vise à harmoniser les règles établies des États membres concernant les systèmes basés sur l'IA. La proposition de règlement énonce des règles axées sur trois catégories de risques (inacceptable, élevé et faible/minimal) et prévoit de couvrir l'utilisation des systèmes d'IA. Elle vise également à compléter les règles et obligations énoncées dans le RGPD et la Directive Police Justice.

CHAPITRE 5 : Évolution politique et principaux points de désaccord

- Quatre positions principales sur les systèmes RBI ont émergé parmi les acteurs politiques à la suite des développements techniques dans le domaine et de l'activité législative précoce des institutions européennes : 1) la promotion active ; 2) le soutien assorti de garanties ; 3) le moratoire et 4) l'interdiction pure et simple.
- Les partisans du soutien assorti de garanties font valoir que le déploiement des technologies RBI doit être strictement surveillé en raison des risques potentiels qu'elles présentent, y compris le danger potentiel de la FRT, de contribuer, par exemple, à criminaliser ou à stigmatiser davantage des groupes de personnes déjà victimes de discrimination.
- Le Parlement européen a adopté une résolution sur l'intelligence artificielle en janvier 2020 dans laquelle il invite la Commission à "évaluer les conséquences d'un moratoire sur l'utilisation des systèmes de reconnaissance faciale". S'il est acté, un tel moratoire pourrait avoir un impact sur certaines utilisations existantes de la FRT, notamment son déploiement dans les espaces publics par les autorités publiques.
- Un certain nombre d'ONG européennes et nationales ont appelé à une interdiction pure et simple de l'utilisation de la FRT, certaines affirmant que le traitement massif de données biométriques provenant d'espaces publics crée un risque sérieux de surveillance de masse qui porte atteinte aux droits fondamentaux.
- La proposition législative de la Commission européenne pour une loi sur l'intelligence artificielle (CE 2021) est à la fois une proposition de cadre réglementaire sur l'IA et un plan coordonné pour soutenir l'innovation. L'une des caractéristiques de cette loi est l'établissement de restrictions en fonction du risque qui s'appliqueraient aux différentes utilisations des systèmes d'IA.

CHAPITRE 6 : Caméras de reconnaissance faciale à l'aéroport international de Bruxelles (Belgique)

- La Belgique est l'un des deux pays européens qui n'a pas encore autorisé l'utilisation de la FRT, cependant, les forces de l'ordre plaident fortement pour son utilisation et les obstacles juridiques actuels à sa mise en œuvre ne devraient pas tenir très longtemps.
- En 2017, à l'insu de l'organe belge de surveillance des informations policières (COC), l'aéroport international de Bruxelles a acquis 4 caméras connectées à un logiciel de reconnaissance faciale pour être utilisées par la police de l'aéroport. Bien que la COC ait par la suite jugé que cette utilisation ne relevait pas des conditions d'un déploiement légal, la

légalité de l'expérience de l'aéroport est tombée dans une zone grise juridique en raison des manières dont la technologie a été déployée.
- Le commissaire général de la police fédérale a justifié la légalité de l'expérience de l'aéroport en comparant le déploiement technologique à l'utilisation légale d'autres technologies intelligentes telles que la reconnaissance automatique des plaques minéralogiques (RAPI). Bien que cet argument ait été rejeté à l'époque, un tel système pourrait être remis en place si les motifs d'interruption ne sont plus présents dans la loi.
- Il existe un mouvement émergent de la société civile en Belgique qui conteste la légitimité de l'identification biométrique à distance. Toutefois, les amendements à la loi sur la police autorisant l'utilisation de caméras intelligentes en temps réel par la police dans l'exercice de ses fonctions administratives et judiciaires, ainsi que les récentes déclarations du précédent ministre de l'Intérieur belge semblent aller dans le sens d'une plus grande acceptation de la surveillance biométrique à distance.

CHAPITRE 7 : Le quartier sans cambriolage de Rotterdam (Pays-Bas)

- Le Fieldlab Burglary Free Neighbourhood est une collaboration public-privé qui a deux objectifs : détecter les comportements suspects et influencer le comportement du suspect. Si le système de lampadaires intelligents recueille certaines données basées sur l'image et le son, il n'enregistre aucune caractéristique propre à l'individu.
- D'un point de vue juridique, la question se pose de savoir si les données traitées par le programme "Quartiers sans cambriolage" peuvent être considérées comme des données à caractère personnel et relèvent donc de la législation sur la protection des données.
- La question de savoir si les formes de surveillance et de signalisation numériques sont réellement les méthodes les plus efficaces pour prévenir les effractions est contestée. Malgré les objectifs du programme, à ce jour, les lampadaires n'ont été utilisés que pour capturer des données à des fins d'apprentissage automatique.
- L'infrastructure installée pour les expériences peut potentiellement être utilisée pour des formes de surveillance plus invasives. Au cours du projet, la police locale, par exemple, a déjà fait part de son intérêt pour l'accès aux caméras.
- L'essai Fieldlab a pris fin en mars 2021. Les données recueillies au cours du projet n'étaient pas suffisantes pour que l'ordinateur puisse distinguer des trajectoires suspectes. L'infrastructure de caméras et de microphones est actuellement désactivée, mais reste en place.

CHAPITRE 8 : Les projets Safe City à Nice (France)
- Plusieurs villes françaises ont lancé des projets de "ville sûre" faisant appel aux technologies biométriques, mais Nice est sans doute le leader national. La ville possède actuellement la plus grande couverture de vidéosurveillance de toutes les villes de France et compte plus du double d'agents de police par habitant que la ville voisine de Marseille.
- Grâce à une série de partenariats public-privé, la ville a lancé un certain nombre d'initiatives utilisant les technologies RBI (notamment la reconnaissance des émotions et du visage). Ces technologies ont été déployées à des fins d'authentification et de surveillance, certaines entrant dans la catégorie de la surveillance biométrique de masse.

- Un projet qui utilisait le RBI dans un lycée de Nice et un autre à Marseille a finalement été déclaré illégal. Le tribunal a estimé que le consentement requis ne pouvait être obtenu en raison du déséquilibre des pouvoirs entre le public visé (les élèves) et l'autorité publique (l'établissement d'enseignement public). Cette affaire met en lumière des questions importantes concernant le déploiement des technologies biométriques dans les espaces publics.
- L'utilisation de la surveillance biométrique de masse par le maire de Nice Christian Estrosi l'a mis en porte-à-faux avec la Commission nationale de l'informatique et des libertés (CNIL) ainsi qu'avec des organisations de défense des droits de l'homme et des droits numériques (Ligue des droits de l'homme, La Quadrature du Net). Ses activités ont suscité à la fois des inquiétudes et des critiques quant à l'utilisation de ces technologies et à leur impact potentiel sur la confidentialité des données personnelles.

CHAPITRE 9 : Reconnaissance faciale à Südkreuz Berlin, Hambourg G20 et Mannheim (Allemagne)

- La police fédérale allemande, en coopération avec la compagnie ferroviaire allemande, a mené un projet appelé "Sicherheitsbahnhof" à la gare de Berlin Südkreuz en 2017/18, qui comprenait 77 caméras vidéo et un système de gestion vidéo.
- La police de Hambourg a utilisé le logiciel de reconnaissance faciale Videmo 360 lors des manifestations contre le sommet du G20 en 2017. La base de données comprend 100.000 individus présents à Hambourg pendant le sommet du G20 et dont les profils sont enregistrés dans la base de données de la police. La technologie permet de déterminer le comportement, la participation à des rassemblements, les préférences et l'engagement religieux ou politique.
- Soixante-huit caméras ont été installées par la police locale sur des places et des lieux centraux de la ville allemande de Mannheim pour enregistrer les schémas de déplacement des personnes. Dans ce projet, qui a débuté en 2018, le logiciel est utilisé pour détecter les comportements suspects.
- La moitié de ces déploiements (Mannheim & Berlin Südkreuz) ont eu lieu en tant que mesures visant à tester l'efficacité des logiciels de reconnaissance faciale et d'analyse comportementale. Cette approche de "justification en tant que test" est souvent utilisée en Allemagne pour justifier un écart par rapport aux règles existantes et aux attentes de la société et a été appliquée de la même manière lors des écarts par rapport aux mesures convenues lors de la pandémie de Coronavirus/COVID-19.
- La résistance à la vidéosurveillance est aussi en grande partie le résultat de campagnes et de protestations constantes de la société civile allemande. Les organisations non gouvernementales Chaos Computer Club et Digital Courage ont toujours fait campagne contre la vidéosurveillance et toute forme de surveillance biométrique ou comportementale. L'effet à long terme de ces projets "pilotes" est de normaliser la surveillance.

LES VERTS/ALE au Parlement européen

25.10.2021

CHAPITRE 10 : Le projet Dragonfly (Hongrie)

- Le gouvernement hongrois dirigé par le Premier ministre Viktor Orbán est depuis longtemps en conflit avec les institutions européennes au sujet de l'État de droit et de la remise en cause de l'indépendance judiciaire et des institutions démocratiques du pays.
- La Hongrie fait figure de pionnier en Europe lorsqu'il s'agit d'autoriser l'utilisation par les forces de l'ordre de la technologie de reconnaissance faciale, de développer une base de données nationale et centralisée (le projet Dragonfly) et d'utiliser l'application de quarantaine à domicile dans le cadre des mesures gouvernementales contre le coronavirus.
- L'infrastructure en place, qui permet potentiellement un déploiement centralisé des technologies biométriques de surveillance de masse en Hongrie, a atteint une ampleur sans précédent, alors que l'examen juridique et éthique de ces technologies accuse un retard dangereux.
- Cela est dû (1) au chevauchement entre les secteurs privé et public, notamment les institutions gouvernementales, et (2) à l'enchevêtrement complexe des systèmes biométriques avec d'autres systèmes d'information (tels que les registres des véhicules, la gestion du trafic, le contrôle et la surveillance des transports publics, etc.)
- Bien que ces derniers ne soient pas concernés par des données relatives au corps humain, ils peuvent néanmoins être utilisés pour la surveillance biométrique de masse et la faciliter. Ces enchevêtrements créent des zones grises de surveillance biométrique de masse où le développement et le déploiement de ces technologies échappent à la visibilité et à l'examen critique.
- Le projet Dragonfly a suscité de nombreuses mises en garde concernant la protection des données et le droit à la vie privée de la part d'organisations publiques et privées. Cependant, l'absence de contestation et de débat social autour des questions de la vie privée et des droits de l'homme dans le cadre de projets tels que le projet Dragonfly du gouvernement hongrois est frappante.