Avis de la Ligue des Droits Humains

sur la proposition de résolution du 16 juin 2020 pour la mise en place d'un moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de sécurité, fixes ou mobiles, dans les endroits publics et privés - DOC 55 1349/011

Janvier 2022

A l'attention de la Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives de la Chambre des représentants.

Objet

La proposition de résolution soumise par la Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives de la Chambre des représentants demande au gouvernement fédéral :

1. de mettre en place un moratoire de trois ans sur l'utilisation de logiciels et d'algorithmes de reconnaissance faciale sur les caméras de sécurité, fixes ou mobiles, dans les endroits publics et privés;
2. de mettre en place un débat à la Chambre des représentants sur ce sujet sensible, pour que cette technologie intrusive ne puisse être implémentée qu'à condition d'être accompagnée de garanties strictes concernant les droits humains.

Introduction

Votre courrier du 25 novembre dernier adressé à la Ligue des Droits Humains (LDH) a retenu toute notre attention. Nous saluons une fois encore la volonté de la Commission de s'entourer d'avis extérieurs dans le cadre de ses travaux et vous remercions pour la confiance dont votre consultation témoigne à notre égard.

Dans son principe, la proposition à l'examen recueille notre soutien. Elle a le mérite de pointer les risques encourus par un déploiement massif de technologies dont les impacts sur nos droits fondamentaux sont inconnus, en ce qu'ils n'ont pas fait l'objet d'une évaluation, et suggère qu'un moratoire soit mis en place afin de permettre un débat parlementaire sur la question de l'utilisation de la reconnaissance faciale.

Dans le même sens, depuis le 1er décembre 2021, l'Italie a instauré un moratoire sur les systèmes de

vidéosurveillance utilisant des technologies de reconnaissance faciale[1]. Ce moratoire est une réalisation importante : il reconnaît les dangers posés par des technologies telles que la reconnaissance faciale pour les droits et libertés des personnes et introduit une interdiction temporaire pour les entités privées d'utiliser ces systèmes dans les lieux publics ou accessibles au public. Le moratoire sera en vigueur jusqu'au 31 décembre 2023, à moins qu'une nouvelle loi ne soit introduite en matière de surveillance biométrique avant cette date.

Parallèlement à cette initiative italienne mettant en place un moratoire sur l'utilisation, par les organismes privés, de la reconnaissance faciale dans certains lieux, au niveau européen est discutée une proposition de Règlement concernant l'Intelligence Artificielle (IA), laquelle prévoit d'instaurer des règles relatives au développement, à la commercialisation et à l'utilisation de tels systèmes. La technologie de reconnaissance faciale étant un type de système d'intelligence artificielle parmi d'autres, la mise en œuvre de règles nationales régulant son usage devrait tenir compte du cadre européen, plus large.

En effet, force est de constater que les systèmes IA – y compris de reconnaissance faciale − sont principalement développés par des organismes privés. Or, la plupart du temps, les pouvoirs publics recourent à ces organismes plutôt que de développer leurs propres outils et solutions en interne, tant pour des raisons de coûts, que d'expertise ou d'efficacité dans leur mise en place. Cependant, cela n'est pas sans conséquences: en vendant des produits directement prêts à l'emploi, les entreprises fournissent des outils dont le fonctionnement et l'articulation sont souvent incompris par leurs destinataires. Il existe dès lors le risque de voir naître une dépendance d'un service public à l'égard d'un opérateur commercial, d'une part, mais aussi un déficit de transparence à l'égard des individus auxquels vont s'appliquer ces outils, d'autre part. Sans oublier le fait que ces logiciels ont une tendance à "susciter leur propre validité" en "pré-formatant la réalité"[2].

C'est la raison pour laquelle la présente proposition, en organisant un moratoire sur le recours à la technologie de reconnaissance faciale, permet d'organiser un débat démocratique indispensable sur ces évolutions et, partant, de questionner la société et les "réalités" que nous voulons pour le futur. Néanmoins, malgré un soutien quant au principe, quelques points posent question et appellent à la clarification. C'est dans cette perspective qu'il convient de prendre connaissance du présent avis.

Champ d'application

Telle que rédigée, la proposition de résolution ne permet pas de savoir avec précisions le champ d'application des usages qu'elle vise à suspendre. Il conviendrait de clarifier certaines notions ainsi que de viser expressément les législations concernées par ce moratoire.

Dans les points suivants, nous énumérons certaines notions qui mériteraient d'être clarifiées :

- Reconnaissance « faciale » : La proposition de moratoire ne concerne que la technologie de reconnaissance faciale. Pourtant, d'autres technologies biométriques ont un impact intrusif similaire. Pensons notamment aux caméras/senseurs permettant d'identifier/authentifier des personnes sur base d'autres modalités biométriques telles que l'iris, les paramètres anthropométriques (analyse de la manière de marcher), les réseaux veineux, etc. Il nous semble important de ne pas réduire le champ d'application de la proposition à l'une des technologies biométriques existantes.

- Caméras de « sécurité » : La proposition de moratoire ne concerne que les caméras

[1] https://edri.org/our-work/italy-introduces-a-moratorium-on-video-surveillance-systems-that-use-facial-recognition/
[2] X. Raufer "Police prédictive : les belles histoires de l'Oncle Predpol", *Sécurité globale*, 2015, p. 101.

de « sécurité ». De telles caméras sont actuellement régies par la loi du 21 mars 2018 et ne visent que les caméras ayant pour finalités de « prévenir, constater ou déceler des infractions contre les personnes ou les biens » et de « prévenir, constater ou déceler des incivilités au sens de l'article 135 de la nouvelle loi communale, contrôler le respect des règlements communaux ou maintenir l'ordre public ». Les caméras de « sécurité » n'englobent donc pas les caméras installées à des fins de contrôles d'accès aux lieux et bâtiments. Par conséquent, le moratoire envisagé ne s'appliquerait pas à l'utilisation de la reconnaissance faciale pour de tels usages. Il nous semble pourtant opportun de prévoir des règles strictes pour l'usage de la reconnaissance faciale à des fins de contrôle d'accès car de tels objectifs peuvent entraîner des conséquences graves et discriminatoires pour les personnes concernées. De telles règles pourraient utilement compléter l'application du RGPD à de tels usages.

- Les destinataires du moratoire : En l'état actuel, il n'est pas clair à qui s'adresse ce moratoire : aux entreprises et particuliers, au secteur public, aux services de police, aux services de la migration, aux services de renseignements ? Pour la LDH, il est évident que ce moratoire s'adresse à toutes ces instances, autorités, personnes physiques et morales. Cela devrait être stipulé *expressis verbis*.

Pour le surplus, étant donnée la volonté de mettre en place un moratoire sur l'utilisation de la technique de reconnaissance faciale (ou plus largement biométrique), il nous semble important, au préalable, de procéder à la réalisation d'un inventaire des normes déjà applicables, de manière générale ou sectorielle. Par exemple, la technologie de reconnaissance faciale est déjà régulée dans le contexte migratoire (e-gates, bases de données SIS, VIS, EES, etc.). La proposition de moratoire remettrait-elle en question de tels usages déjà autorisés par d'autres normes nationales ou européennes ?

Recommandation : A des fins de lisibilité, une liste des usages spécifiques et des législations concernées pour chacun de ces usages pourrait être élaborée.

Reconnaissance faciale et surveillance biométrique

Les termes "reconnaissance faciale" et "reconnaissance biométrique à distance" couvrent un large éventail de technologies, depuis le système d'authentification faciale qui déverrouille le téléphone d'une personne ou autorise l'accès à certains lieux, jusqu'aux technologies d'identification de la démarche d'une personne, de sa voix ou de son système veineux, en passant par les systèmes censés détecter l'identité sexuelle ou l'état émotionnel d'une personne. Il importe de les distinguer pour en cerner les contours.

La biométrie porte sur l'analyse des caractéristiques physiques ou comportementales propres à chaque individu. C'est par le biais de l'intelligence artificielle que les technologies numériques automatiques, telles que la reconnaissance faciale par caméras dans l'espace public, opèrent une surveillance biométrique. Toute surveillance biométrique, c'est-à-dire une reconnaissance des caractéristiques physiques ou comportementales des personnes présentes dans les lieux publics ou accessibles au public, devrait être considérée avec les mêmes précautions en ce qu'elles sont des données à caractère personnel, telles que définies par le 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[3]. Elles y sont spécifiquement définies comme étant les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales

[3] RGPD, Art. 4 (1).

d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.[4] Des entreprises privées œuvrant à la recherche et au développement de mécanisme autrement plus précis et performants que la seule reconnaissance faciale, il s'impose de ne pas s'y limiter.

Recommandation : La LDH encourage vivement l'extension du champ d'application de ce moratoire à tout usage de technologies reposant sur l'utilisation de données biométriques et non pas aux seules technologies de reconnaissance faciale par caméra et aux logiciels qu'elles nécessitent.

Authentification et identification

La proposition évoque indistinctement les questions soulevées tant par les mécanismes d'authentification que d'identification (faciale ou biométrique). La clarification de ce point et la distinction à faire entre ces notions est indispensable à la bonne compréhension de leurs champs d'application.

En effet, l'authentification (c'est-à-dire la correspondance un à un) règle les questions d'accès à des environnements sécurisés, tels que l'accès à des portails de sécurité au contrôle des frontières, nos visages étant scannés et comparés aux données biométriques contenues dans nos passeports, ou encore le déverrouillage d'un téléphone portable par la détection d'une empreinte digitale ou d'une reconnaissance de l'iris de l'œil.

L'utilisation de ces technologies pour identifier ou distinguer une personne d'un ensemble plus large d'individus, également connue sous le nom d'identification faciale ou biométrique (c'est-à-dire établir une correspondance parmi plusieurs personnes) est porteuse d'autres enjeux, en ce qu'elle permet d'identifier, donc d'isoler et suivre des personnes en utilisant leur visage, leur démarche, leur voix, leur apparence personnelle ou tout autre identifiant biométrique, d'une manière qui permette de les identifier.

Ces deux types de technologies, bien que comprenant des avantages en termes purement technologiques, peuvent être construites et utilisées de manière à permettre des formes de surveillance problématiques, par exemple en créant de grandes bases de données biométriques centralisées qui peuvent être réutilisées à d'autres fins. Elles ouvrent la voie à la surveillance de masse ainsi qu'à une surveillance ciblée potentiellement discriminatoire, c'est-à-dire une surveillance qui a un impact disproportionné sur les droits humains et les libertés civiles. Même sous couvert d' « anonymisation » des données d'identité, ces outils impactent les comportements individuels, dictent leurs rapports à l'espace public ainsi qu'à tout espace qui ne peut être évité, les interprètent. C'est pourquoi leur usage ne peut fait l'économie d'un large débat parlementaire et permettre à la société civile d'en comprendre les enjeux.

Recommandation : La LDH est d'avis que le moratoire devrait s'appliquer tant aux processus d'authentification qu'à ceux d'identification biométriques.

Absence de disposition relative à l'usage des images faciales

La loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour, établit les données personnelles récoltées pour chaque individu, en ce compris la photographie et les empreintes digitales. Cette loi prévoit notamment une

[4] Art. 4 (14)

liste d'autorités habilitées à lire l'image numérisée des empreintes digitales de l'index de la main gauche et de la main droite du titulaire de la carte d'identité. Cependant, aucune disposition n'autorise ni ne limite l'accès aux images faciales, lequel peut faire l'objet de législations distinctes dans la poursuite d'autres objectifs.

Les techniques d'authentification utilisent les images faciales pour contrôler l'accès aux espaces. Dans l'espace Schengen par exemple, elles sont notamment utilisées aux postes frontières via le contrôle automatisé des passeports biométriques par les « e-gates » au sein des aéroports. Au niveau national, il n'existe pas d'inventaire des normes interdisant ou autorisant l'usage des techniques de reconnaissance faciale. Un tel inventaire devrait être dressé en tenant compte des conséquences distinctes que l'utilisation de telles techniques emportent dans le chef des autorités publiques et celui des personnes privées.

De plus, la loi caméra, applicable dans le secteur privé et le secteur public, ne s'applique pas aux usages de l'imagerie par ces secteurs à des fins de contrôle d'accès. Rien n'empêche, à ce stade, d'imaginer qu'une entreprise, une administration, voire des personnes privées, s'équipent du matériel permettant d'organiser un accès à certains espaces encadrés par des technologies de reconnaissances biométriques. Tout au plus, la disproportion pourrait être invoquée sur base du RGPD. Le moratoire s'appliquerait-il à ces usages ? Dans l'affirmative, une révision de la loi caméra ne permettrait-elle pas d'encadrer plus strictement de tels usages par les particuliers ?

Se limitant à viser *« les caméras de sécurité, fixes ou mobiles, dans les endroits publics et privés »,* la proposition de résolution n'indique pas le types de caméras visées par le moratoire. S'agit-il de celles utilisées par le secteur public (la police, les services de renseignement, de l'immigration, les communes) et/ou celles utilisées par le secteur privé (les particuliers surveillant leur propriété, les exploitants de lieux ouverts au public tels que les cafés, hôtels, restaurants, magasins…) ? Outre les espaces publics, concerne-t-il indifféremment tous les espaces privés ou uniquement ceux accessibles au public ? S'agit-il d'un moratoire sur l'utilisation uniquement par la police judiciaire ou également la police administrative ? Quelles sont ses implications sur l'application des dispositions actuelles de la loi caméras et de la loi sur la fonction de police ?

Dans ce contexte, la question de l'accès aux données personnelles et de l'exercice des droits RGPD (accès, rectification, effacement, etc.) est particulièrement sensible. La pratique montre que, dans le cadre de la loi caméra, l'exercice de ces droits est particulièrement dysfonctionnel.

Recommandations : La LDH recommande l'établissement d'un inventaire des normes concernant l'usage des techniques de reconnaissance faciale en tenant compte des conséquences distinctes que l'utilisation de ces techniques emportent dans le chef des autorités publiques et celui des personnes privées.
Pour l'heure, la mise en place d'un moratoire généralisé sur l'utilisation de ces technologies assurerait une protection effective des données personnelles. Néanmoins, si ces usages venaient à être autorisés, de nombreuses garanties d'effectivité des droits prévus par le RGPD devraient être instaurées, telles que, par exemple, une autorisation préalable de l'APD basée sur une étude d'impact avant tout recours à une technologie biométrique ainsi que des moyens de contrôle a posteriori tels qu'un droit d'accès aux images, une information du public renforcée, des voies de recours effectives, etc.

L'utilisation par les pouvoirs publics (forces de l'ordre, pouvoir judiciaire)

Dans son avis sur la proposition de loi du 6 avril 2021 modifiant la loi relative à la publicité de l'administration du 11 avril 1994 afin d'introduire une plus grande transparence dans l'usage des algorithmes par les administrations rendu en septembre 2021, la LDH exposait déjà ses craintes quant

à l'usage des algorithmes dans les administrations.[5]

La LDH considère, quel que soit l'usage envisagé, que certaines décisions administratives ne devraient avoir en tout en partie pour fondement un traitement algorithmique. La plus grande vigilance doit prévaloir notamment dans certains domaines, comme par exemple celui des forces de l'ordre et du pouvoir judiciaire dans la politique criminelle (détection, prévention, enquêtes ou poursuites des infractions pénales) ou la politique migratoire, bien trop souvent prétextée pour permettre des expérimentations ou justifier de contrôles violant les droits de ces individus[6].

Dans cet ordre d'idée, des limites claires devraient être prévues, telles que celles contenues, pour exemple et non limitativement, dans l'article 47 de la loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[7] :
- "*Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne.*
- *Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne devrait pouvoir être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel.*
- *Aucune décision par laquelle l'administration se prononce sur un recours administratif mentionné au titre Ier du livre IV du code des relations entre le public et l'administration ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel.*"

Pour le surplus, la LDH renvoie à sa note de septembre 2021.

Recommandations : Pour la LDH, certains usages ne devraient en aucun cas reposer sur des traitements algorithmiques. Le principe de subsidiarité imposant de démontrer que d'autres moyens d'atteindre l'objectif n'existent pas doit prévaloir à tout usage dans le cadre de politiques publiques.

L'utilisation par des personnes privées

Que l'on pense au cas de CLEARVIEW AI Inc., entreprise américaine qui recherche et stocke les photos de visages postées sur internet pour constituer une base de données biométriques, ou à tout usage par des particuliers, de plus en plus de fournisseurs privés de technologies de reconnaissance faciale compilent et amalgament des bases de données d'individus et partagent ces bases de données avec de multiples clients.

En France, la Commission nationale française de l'informatique et des libertés (CNIL) vient de mettre en demeure CLEARVIEW de cesser la collecte et l'usage des données des personnes se trouvant sur le territoire français en l'absence de base légale, de faciliter l'exercice des droits des personnes concernées et de faire droit aux demandes d'effacement formulées, dans un délai de 2 mois.[8] La

[5] Avis de la LDH, sur la proposition de loi du 6 avril 2021 modifiant la loi relative à la publicité de l'administration du 11 avril 1994 afin d'introduire une plus grande transparence dans l'usage des algorithmes par les administrations – septembre 2021 https://www.liguedh.be/avis-de-la-ligue-des-droits-humains-et-de-la-liga-voor-mensenrechten-sur-la-proposition-de-loi-du-6-avril-2021-modifiant-la-loi-relative-a-la-publicite-de-ladministration-du-11-avril-1994-af

[6] Voy. Résolution du Parlement européen du 6 octobre 2021 sur l'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales (2020/2016(INI)), point 31 concernant le projet de recherche iBorderCtrl, visant à déployer un «système intelligent de détection de « mensonges » aux frontières extérieures, afin d'établir le profil des voyageurs sur la base d'un entretien automatisé réalisé par webcam avant le voyage et d'une analyse de 38 micro-gestes fondée sur l'intelligence artificielle : https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_FR.pdf.

[7] Article 47 de la Loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037823131/.

[8] https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-met-en-demeure-clearview-ai-de-cesser-la-reutilisation-de, consulté le 22 décembre 2021.

société de reconnaissance faciale détiendrait plus de trois milliards d'images collectées illégalement sur internet. Des plaintes ont été soumises aux régulateurs de la protection des données en France, en Autriche, en Italie, en Grèce et au Royaume-Uni. La confirmation d'un usage par la police fédérale belge du logiciel Clearview en octobre 2021[9] inquiète.

L'utilisation de ces technologies par des acteurs privés peut constituer la même menace pour nos droits, en particulier lorsque, de par leur ampleur, ces derniers peuvent s'engager effectivement dans la surveillance au nom de partenariats public-privé, tel que celui que propose CLEARVIEW. Cela revient, en pratique, à la création de "bases de données nationales" compilées à la discrétion d'un personnel non formé, qui ne sont soumises à aucune surveillance, qui peuvent être partagées entre des sociétés privées et entraîner une discrimination à l'encontre des personnes soumises à leur usage.

Recommandations : l'utilisation de ces technologies par les personnes privées et les récoltes de données qu'elles entrainent sont d'autant plus dangereuses qu'elles répondent à des logiques marchandes. Leur interdiction devrait être clairement exprimée.

Absence de consensus européen

Les données biométriques tombant dans le champ d'application du Règlement sur la protection des données, le consentement de chaque personne devrait être recueilli en cas de collecte. Ceci est impossible de la part des individus qui se déplacent dans l'espace public. L'inverse constituerait une atteinte à leur liberté de mouvement. Pourtant, les technologies de reconnaissance biométrique sont de plus en plus installées voire utilisées dans l'espace public[10].

En avril 2021, la **Commission européenne** a déposé une proposition de réglementation[11] visant à distinguer les systèmes d'IA « bénéfiques » de ceux qui pourraient poser problème dans le futur. Elle prévoit quatre niveaux de risque correspondant à une utilisation plus ou moins proscrite du système d'IA réglementé : les systèmes à risque minime, limité, élevé ou inacceptable. Seuls les derniers seraient interdits car considérés comme contraires aux valeurs de l'Union : ils recoupent notamment les systèmes de notations sociales par les Etats ou de manipulation des comportements humains visant à priver les utilisateurs de leur libre arbitre ou encore les systèmes d'IA pour l'identification biométrique à distance « en temps réel » dans des espaces accessibles au public à des fins répressives. Les systèmes d'IA utilisés pour des opérations de "surveillance indiscriminée" tomberaient dans la catégorie des systèmes à risques élevés. Cette catégorie implique une interdiction de principe d'utilisation à laquelle il peut être fait exception moyennant le respect de conditions préalables à leur usage et leur mise sur le marché, telles que leur évaluation, la traçabilité des résultats, l'information et la transparence. Déjà, des voix s'élèvent pour mettre en garde que les exceptions ne vident *in fine* l'interdiction de principe de sa substance.

En outre, l**e Comité européen de la protection des données (EDPB)** et **le Contrôleur européen de la Protection des Données (CEPD)** ont adopté un avis conjoint sur l'usage de la reconnaissance faciale

---

[9] https://www.lesoir.be/399086/article/2021-10-06/reconnaissance-faciale-la-police-belge-admet-avoir-utilise-un-logiciel, consulté le 22 décembre 2021.

[10] Voir par exemple Q. Noirfalisse, « Courtrai, la foi dans la caméra », *Médor*, 21/12/2021 https://medor.coop/hypersurveillance-belgique-surveillance-privacy/police-justice-bng/episodes/courtrai-la-foi-dans-la-camera-episode-12-videosurveillance-briefcam/.

[11] Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'union. 2021/0106 (COD) déposé le 21.04.2021, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52021PC0206.

dans les lieux publics)[12] : ils demandent l'interdiction de l'utilisation de l'IA pour la reconnaissance automatisée des caractéristiques humaines dans les espaces accessibles au public (visant les systèmes de reconnaissance des visages, de la démarche et de la posture, des empreintes digitales, de l'ADN, de la voix et de tout autre signal biométrique ou comportemental, quel que soit le contexte, et souhaitant leur interdiction dans les espaces publics). Ces deux organismes ont visé plusieurs points de la réglementation sur l'intelligence artificielle proposée par la Commission européenne, parmi lesquels la nécessité de préciser explicitement que la législation européenne existante en matière de protection des données (RGPD, EUDPR, LED) s'applique à tout traitement de données personnelles entrant dans le champ d'application de la réglementation sur l'IA, ainsi que la désignation des APD comme autorités nationales de surveillance et des garanties d'autonomie et d'indépendance de l'organe européen chargé des questions relatives à l'IA.

Dans son avis sur la proposition de règlementation européenne sur l'intelligence artificielle[13], la CNIL, quant à elle, ajoute à ces observations quelques points fondamentaux dans la mise en place d'un règlement européen sur l'IA. Elle recommande tout d'abord d'élargir le champ des systèmes d'IA interdits et de clarifier leur définition. Elle préconise ensuite de veiller à ce que cette réglementation soit en accord avec le règlement général sur la protection des données (RGPD), l'enjeu majeur étant l'articulation du règlement sur l'intelligence artificielle avec le RGPD et la directive « Police-Justice ». Elle pointe ensuite la nécessité d'une gouvernance harmonisée de l'intelligence artificielle par le Comité européen de l'intelligence artificielle (CEIA) ainsi que des garanties d'indépendance et un renforcement de ses pouvoirs afin de lui permettre d'exercer un véritable contrôle, notamment lors de la mise en œuvre de systèmes d'IA à l'échelle européenne. Elle propose enfin que les autorités de protection des données soient désignées comme autorités de contrôle national de l'intelligence artificielle.

En octobre 2021, **le Parlement européen** a adopté une résolution sur l'usage de l'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales[14]. Elle demande notamment l'interdiction permanente de l'utilisation de l'analyse et/ou de la reconnaissance automatisées, dans les espaces accessibles au public, d'autres caractéristiques humaines telles que la démarche, les empreintes digitales, l'ADN, la voix et d'autres signaux biométriques et comportementaux[15]. En outre, elle demande un moratoire sur le déploiement des systèmes de reconnaissance faciale à des fins répressives destinés à l'identification, à moins qu'ils ne soient utilisés qu'aux fins de l'identification des victimes de la criminalité, jusqu'à ce que les normes techniques puissent être considérées comme pleinement respectueuses des droits fondamentaux, que les résultats obtenus ne soient ni biaisés, ni discriminatoires, que le cadre juridique offre des garanties strictes contre les utilisations abusives ainsi qu'un contrôle et une surveillance démocratiques rigoureux, et que la nécessité et la proportionnalité du déploiement de ces technologies soient prouvées de manière empirique[16]. Il est en outre précisé que lorsque les critères susmentionnés ne sont pas remplis, les systèmes ne devraient pas être utilisés ou déployés.

Au sujet de l'usage éventuel de bases de données privées de reconnaissance faciale, telles que Clearview AI, par les services répressifs et les services de renseignement, la résolution invite les États membres à les obliger à faire savoir s'ils utilisent des technologies équivalentes et rappelle que le Comité européen de la protection des données a estimé que l'utilisation d'un service comme celui-ci

---

[12] Avis conjoint 05/2021 du 18 juin 2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_fr.pdf.

[13] https://www.cnil.fr/fr/intelligence-artificielle-lavis-de-la-cnil-et-de-ses-homologues-sur-le-futur-reglement-europeen

[14] Résolution du Parlement européen du 6 octobre 2021 sur l'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales (2020/2016(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_FR.pdf.

[15] *Ibid*, point 26.

[16] *Ibid*. point 27.

par les autorités répressives dans l'Union « ne serait probablement pas compatible avec le régime de protection des données de l'Union ». L'interdiction de l'utilisation des bases de données privées de reconnaissance faciale dans le domaine répressif est demandée sans équivoque[17].

Ces informations montrent à suffisance que le débat n'est pas abouti au niveau européen et qu'en l'attente d'une réglementation, les risques pour les libertés fondamentales engendrés par l'utilisation par l'IA de données biométriques, dans les espaces accessibles au public, sont indéniables.

Déjà, il apparaît que certaines utilisations de la surveillance biométrique de masse dans les États membres et par des agences de l'UE ont donné lieu à des violations de la législation de l'UE en matière de protection des données et ont indûment restreint les droits des personnes, y compris le droit au respect de la vie privée, le droit à la liberté d'expression, le droit de manifester et le droit à la non-discrimination. Le recours généralisé à la surveillance biométrique, au profilage et à la prédiction constitue une menace pour l'état de droit et pour nos libertés les plus fondamentales.

Du côté de la société civile, la campagne Reclaim your face[18], une initiative citoyenne européenne (ICE) lancée par EDRI (European Digital Rights) en 2021 lance a recueilli le soutien de 40 organisations dont celui la LDH. Ensemble, elles ont exhorté la Commission européenne à réglementer strictement l'utilisation des technologies biométriques afin d'éviter toute atteinte injustifiée aux droits fondamentaux. En particulier, l'interdiction, en droit et en pratique, des utilisations indifférenciées ou arbitrairement ciblées de la biométrie pouvant conduire à une surveillance de masse illégale est demandée. Susceptibles d'entraîner une atteinte inutile ou disproportionnée aux droits fondamentaux des personnes, ces systèmes intrusifs ne devraient être développés, mis en place (même à titre expérimental) ou utilisés par des entités publiques ou privées. Par cette ICE, les organisations prient donc instamment la Commission de proposer un acte juridique qui s'appuiera sur les interdictions générales prévues par le Règlement général de protection des données (RGPD) et la directive en matière de protection des données dans le domaine répressif et respectera pleinement lesdites interdictions, pour faire en sorte que le droit de l'Union interdise explicitement et spécifiquement la surveillance biométrique de masse.

Recommandation : Conscient de ces enjeux et des usages illégaux déjà constatés, l'Etat belge devrait s'engager fermement sur la voie de l'interdiction de ces usages, quelle que soit la position européenne.

Conclusions

A l'heure actuelle, aucune loi n'interdit expressément l'usage de caméras de surveillance intelligentes à des fins de reconnaissance faciale en Belgique. Il serait toutefois naïf d'affirmer que l'interdiction l'emporterait *de facto* dès lors que les dispositifs de surveillance, précédemment autorisés et déployés dans l'espace public, font régulièrement l'objet de renouvellements en faveur d'un matériel de plus en plus performant et incluant déjà ces technologies. Entreprises privées et consommateurs, mais également les services publics produisent et/ou achètent des objets que les réglementations peinent à encadrer suffisamment rapidement. La prééminence des enjeux économiques du marché de la surveillance doit être prise en compte dans l'analyse des discours de la normalisation des techniques de vidéosurveillance s'exerçant dans les espaces et sur l'acceptabilité sociale de la sécurité[19].

Si un moratoire sur ces usages paraît devoir s'imposer au regard des dangers que ces usages représentent pour nos sociétés, la LDH plaide pour leur interdiction de principe.[20]

---

[17] *Ibid*, point 28.
[18] Reclaim your face, https://reclaimyourface.eu/fr/
[19] LEMAIRE E., *L'œil sécuritaire. Mythes et réalité de la vidéosurveillance.* Paris, La Découverte, 2019.
[20] https://www.liguedh.be/initiative-de-la-societe-civile-en-vue-dune-interdiction-des-pratiques-de-surveillance-biometrique-de-masse/